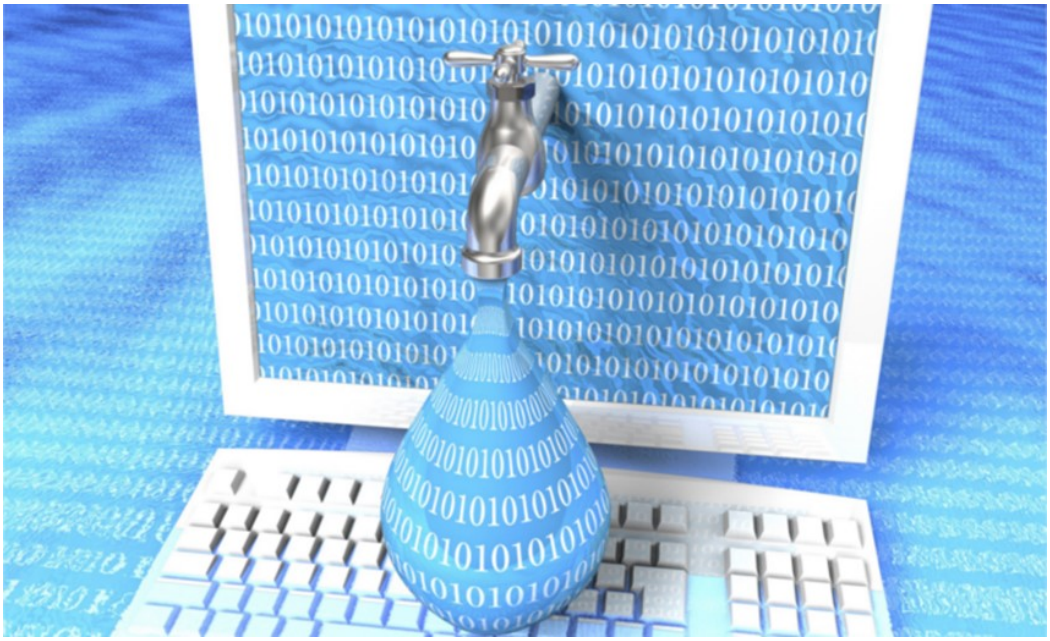
Uitwerking Informatiebeveiligingsbeleid 2022

gemeente Nijmegen



Versiebeheer

Het versiebeheer van dit document ligt bij de CISO.

Kenmerk:	E22.000032
Versie:	1.0
Versiedatum:	Januari 2022
Documentnaam:	Uitwerking Informatiebeveiligingsbeleid 2022
Portefeuillehouder	Petra Molenaar
Classificatie:	openbaar

Inhoudsopgave

Inleiding

Waarom Informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie is essentieel voor een gemeente omdat het de basis is voor juist en efficiënt handelen. Gemeente Nijmegen wil zich verantwoordelijk gedragen, aanspreekbaar en servicegericht zijn. Gemeente Nijmegen wil bovenal transparant en proactief verantwoording afleggen aan burgers en raadsleden en met minimale middelen maximale resultaten behalen. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe strenger de maatregelen die getroffen moeten worden. Waarde van informatie kan bestaan uit de schade die verlies oplevert voor een burger op het moment dat persoonsinformatie niet meer onder controle staat van de gemeente. Maar waarde kan ook bestaan uit de impact van een politiek gevoelig lek, of financieel gewin door voorkennis op inkoop trajecten of speculaties op grond transacties.

Wat is Informatiebeveiliging?

Informatiebeveiliging gaat over het treffen van maatregelen om de betrouwbaarheid van werkprocessen, gebruikte applicaties en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen van buitenaf. Specifieker gaat het om ervoor te zorgen dat:

- beschikbaarheid/continuïteit: informatie op de juiste tijd en plaats beschikbaar is voor gebruikers.
- vertrouwelijkheid (privacy): informatie alleen toegankelijk is voor bevoegden en onbevoegden vertrouwelijke informatie niet kunnen inzien of aanpassen.
- betrouwbaarheid: informatie juist, volledig, tijdig en de verwerking controleerbaar is
- duurzaamheid: informatie tijdig gearchiveerd wordt zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft (bron: archiefwet)

Het gaat niet alleen over ICT. Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.[1] Integriteit en de bescherming van onze informatiestromen gaan hand in hand.

Op dit gebied zijn best practices beschreven. Deze standaarden zijn vastgelegd in normen. De bekendste norm op dit terrein is de ISO 27001/2 norm. De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor de Nederlandse overheid, gebaseerd op de ISO 27001/2 norm. Afkortingen zijn terug te vinden in de begrippenlijst in hoofdstuk 18.

Wat is de reikwijdte van Informatiebeveiliging?

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om:

1. alle *uitingsvormen* van informatie (in woord, beeld of geluid)
2. alle mogelijke *informatiedragers* (op papier of elektronisch)
3. alle informatie verwerkende *systemen* (hardware en software)

Maar vóóral ook om mensen en processen.

Uit onderzoek blijkt dat de meeste incidenten niet voortkomen uit een gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Maatregelen op het gebied van informatiebeveiliging beperken zich dan ook niet alleen tot technische maatregelen. Denk bijvoorbeeld aan:

- het invoeren van een *'clean desk'*-beleid. Immers, een opgeruimd bureau verminderd de kans dat gevoelige en officiële documenten rondslingeren en daardoor in verkeerde handen terechtkomen.
- het opstellen van regels over de omgang met mobiele devices (laptops, telefoons), om er voor te zorgen dat de informatie die medewerkers bij zich dragen net zo goed beschermd is als die in het stadhuis.
- het geven van aanwijzingen voor telewerken, over bijvoorbeeld het delen van informatie tijdens online vergaderingen.

[1] *Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een organisatie verricht.*

Waarom dit beleidsdocument?

Dit document is een algemene uitwerking van beleid op het vlak van informatiebeveiliging. Deze uitwerking levert uitgangspunten op en regels die de keuzes van gemeente Nijmegen weergeven op het vlak van informatiebeveiliging. Deze keuzes zijn gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Zij leiden tot het best passende beleid voor Nijmegen.
In dit document zijn de beleidsuitgangspunten per BIO hoofdstuk nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteitshandhaving van de) bedrijfsvoering. Ook voor privacy is een dergelijke beheerstructuur van belang. De overlap bevindt zich op het vlak van de juiste organisatorische en technische maatregelen ter bescherming van de persoonsgegevens, zoals bedoeld door de AVG. De beheerstructuren overlappen daarom met elkaar. Voor aanvullingen op het vlak van privacy, zie het geldende Privacy Beleid van gemeente Nijmegen zoals vastgesteld door het college van Burgemeester en Wethouders.

De informatiebeveiligingsmaatregelen worden per BIO hoofdstuk verder uitgewerkt in dit document Uitwerking Informatiebeveiligingsmaatregelen, dat tegelijk met het Informatiebeveiligingsbeleid door het GMT is vastgesteld. Dit informatiebeveiligingsbeleid omvat tevens het beveiligingsplan voor de uitvoering wet werk en inkomen (Suwinet).

Wat zijn de pijlers onder het informatiebeveiligingsbeleid van Nijmegen?

Het bestuur en (lijn)management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid[2]. Het management geeft richting aan het informatiebeveiliging en laat zien dat zij informatiebeveiliging belangrijk vindt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid. Dit beleid is van toepassing op de gehele organisatie: alle processen, organisatieonderdelen, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving.

De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Met de volgende randvoorwaarden:

- Wetgeving waar aan voldaan moet worden. Denk bijvoorbeeld aan wetgeving op het vlak van stelsels met persoonsgegevens, geografische gegevens en privacy wetgeving[3].
- We hebben landelijk als basis een gemeenschappelijk normenkader: de Baseline Informatiebeveiliging Overheid (BIO). De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering bij het maken van risico-analyses.
- Daarnaast werken we met de tien bestuurlijke principes voor informatiebeveiliging (opgesteld door de VNG) in aanvulling op de Baseline.

Dit leidt tot de volgende 10 uitgangspunten die in de rest van dit uitwerkingen document verder worden toegelicht:

1. De eindverantwoordelijkheid voor de informatiebeveiliging ligt bij het **College van B&W**, maar informatiebeveiliging is van iedereen. Het bestuur geeft het goede voorbeeld.
2. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt, samen met het systeem waarin de ontwikkeling en de planning van de maatregelen wordt beheerd (het ISMS), de basis voor een betrouwbare informatievoorziening. De prioriteit in het ISMS wordt oa bijgesteld op basis van risico management.
3. Informatiebeveiliging is een **continu verbeterproces** dat zich steeds aanpast aan veranderende omstandigheden. De plan-do-check-act-cyclus vormen samen het **managementsysteem** van informatiebeveiliging.
4. Het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging gebeurt op basis van **Kritieke Prestatie Indicatoren (KPI`s)**.
5. We kennen de volgende **functies** rondom informatiebeveiliging,

[2] Deze rol wordt nader uitgewerkt in het zogeheten “three lines of defense’-model zoals dat beschreven wordt verder op in dit document.

[3] Wetgeving als BRP, SUWI, BSN, BAG/BGT/BRO en PUN, maar ook de archiefwet. En Europese wetgeving zoals de GDPR.

- CISO: Chief Information Security Officer, informatiebeveiligingsfunctionaris (gemeentebreed)
- FG: Functionaris Gegevensbescherming (gemeente breed)
- Voor Suwinet: Security Officer
- Voor de basisregistratie personen (BRP): beveiligingsbeheerder BRP
- Voor de reisdocumenten: beveiligingsfunctionaris Reisdocumenten
- Voor de rijbewijzen: beveiligingsfunctionaris Rijbewijzen

In de Uitwerking Informatiebeveiligingsmaatregelen worden deze rollen nader omschreven.

6. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen. Informatiebeveiliging kost geld.
7. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van de voor hen relevante procedures.
8. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken bij de CISO.
9. Onze informatiebeveiliging heeft invloed op en wordt ook geraakt door die van onze ketenpartners.
10. Wij registreren onze incidenten en leren daarvan zodat onze ervaringen ons weerbaarder maken.

Uitwerking Informatiebeveiligingsmaatregelen

De toegepaste hoofdstukken uit de BIO norm zijn:

6 Beheer van de Interne Organisatie
7 Beheer van bedrijfsmiddelen;
8 Beveiliging van personeel;
9 Fysieke beveiliging en beveiliging van de omgeving;
10 Beheer van communicatie- en bedieningsprocessen;
11 Toegangsbeveiliging;
12 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
13 Beheer van informatiebeveiligingsincidenten;
14 Bedrijfscontinuïteitsbeheer;
15 Naleving
17 Beveiligingsbeleid gebruik Suwinet

De nummering van de hoofdstukken in dit document komt overeen met de BIO norm om de onderlinge relatie te verduidelijken. De informatie over Suwinet is op advies van het Ministerie van Sociale Zaken gebundeld in een apart hoofdstuk. De gebruikte afkortingen zijn terug te vinden in de begrippenlijst in hoofdstuk 18.

6. Beheer van de Interne Organisatie – organisatie van rollen en verantwoordelijkheden

Hoe zijn rollen en verantwoordelijkheden georganiseerd?

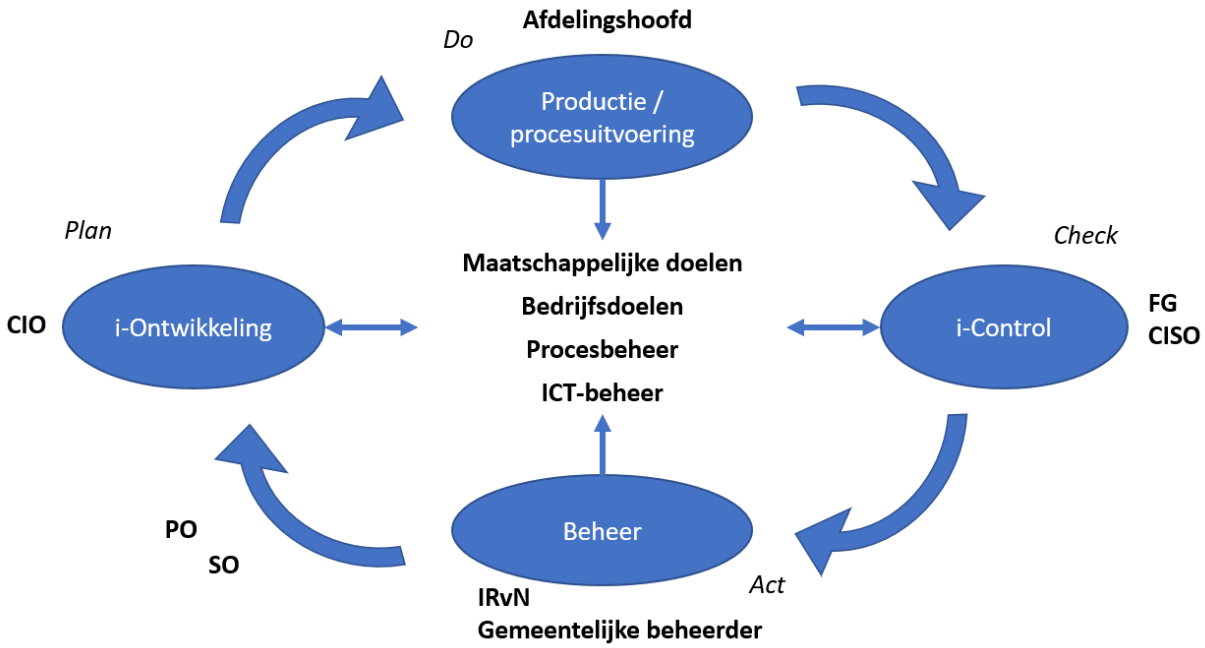
Aanvullend op de baseline vraagt veranderende wetgeving extra maatregelen van de gemeente. In het geval van het beleggen van verantwoordelijkheden springt het benoemen van een FG in het oog. De AVG stelt dit verplicht voor alle overheidsorganisaties.

Op hoofdlijnen kunnen er 4 verschillende beheersingsrollen rond informatievoorziening en de wijze van besturen onderscheiden worden. Twee van deze rollen vormen een uitvoerende kern van de organisatie:

- **Productie** = zorgdragen voor producten en diensten, behalen van maatschappelijke doelen
- **Beheer** = ondersteunen van productie en zorgen voor randvoorwaarden om maatschappelijke doelen te halen

De andere 2 rollen vormen de “technostructuur” van de organisatie, de staffunctie van de organisatie. Zij voeren niet uit, maar adviseren, controleren, zijn gericht op het bepalen van maatschappelijke en bedrijfsdoelen en het bewaken dat deze doelen gehaald worden.

- **i-Control** = controleren, signaleren, verantwoorden --> beheersen vanuit verantwoording/compliancy
- **i-Ontwikkeling** = innoveren, visie bepalen, ontwikkelen --> beheersen vanuit visie en strategie



Figuur 1: beheersingsrollen in relatie

Hoe passen we Three Lines of Defence toe?

Een tweede model dat van belang is voor met name de beheersing van risico's, is het "Three Lines of Defence" -model. Dit model gaat uit van de volgende principes:

1. Afdelingen (en daarbinnen hoofden en medewerkers) die in directe zin verantwoordelijk zijn voor de realisatie van de strategie en voor de daarvan afgeleide doelstellingen zijn daarmee ook primair verantwoordelijk voor het managen van de risico's die met de eigen bedrijfsvoering samenhangen;
2. Afdelingen (en daarbinnen hoofden en medewerkers) die verantwoordelijk zijn voor de structuur en inrichting van de organisatie en een meer indirecte verantwoordelijkheid hebben realisatie van de strategie en voor de daarvan afgeleide doelstellingen zijn ondersteunen de bovenstaande afdelingen bij het identificeren en bewaken van risico's. Deze vormen de tweede lijn van verdediging.
3. De derde lijn in het model staat voor de interne auditfunctie: deze voorziet de hoogste leiding van aanvullende zekerheid over de kwaliteit van sturing en beheersing.

	Beheersingsrol	Afdelingen
1e lijn	Productie/procesuitvoering + Beheer	Lijnafdelingen, uitvoerende beheer-en stafafdelingen
2e lijn	i-Ontwikkeling + i-Control + Beheer	Stafafdelingen, beheerafdelingen
3e lijn	i-Control	Stadscontrol

Afdelingen binnen de gemeente hebben taken vanuit een of meerdere beheersingsrollen en "lines of defence". Zo hebben afdelingen die als 'lijnafdeling' te boek staan vooral een productierol en zitten daarmee in de eerste linie van beheersing, maar deze afdelingen kunnen ook elementen uit de control, beheer en ontwikkelingsrol in zich hebben en daarmee ook 2e lijns 'verdediging' ingebouwd hebben. Beheerafdelingen kunnen ook ontwikkelings- en control-taken in zich hebben, vooral op specifieke technische gebieden. Een onderscheid zoals deze hieronder voor de verschillende betrokken afdelingen gegeven wordt, moet met deze nuance gelezen worden.

1. **Medewerker** - Informatiebeveiliging en zorgvuldige omgang met (persoons)gegevens is ieders verantwoordelijkheid. Iedere medewerker, zowel vast als tijdelijk, intern of extern kent de waarde van informatie waar mee omgegaan wordt (voor de gemeente en andere betrokkenen) en handelt daarnaar. Van hen wordt verwacht dat ze actief bijdragen aan de veiligheid van informatie en informatiesystemen en bij vermeende inbreuken hierop (informatiebeveiligingsincidenten) hiervan melding te maken. Er wordt van alle medewerkers verwacht dat ze zich 'fatsoenlijk' gedragen en als de zaak er om vraagt geheimhouding betrachten. Zij worden hierin ondersteund door de gemeente Nijmegen.

   Medewerkers gebruiken informatie alleen voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt. Zij beschermen de integriteit en goede naam van de gemeente. Medewerkers zijn binnen 3 maanden na in dienst zijn opgeleid in het gebruik van informatiesystemen en andere informatiebronnen en weten wat van hen verwacht wordt in het kader van informatiebeveiliging en privacybescherming. De kennis hier van wordt aangereikt door algemene communicatie over beveiligingsrichtlijnen en bewustwordingsactiviteiten, als ook door training.

2. Een **manager** - waaronder ieder hoofd of teamleider - is (mede-)verantwoordelijk voor de integrale informatiebeveiliging van en privacybescherming binnen zijn of haar organisatieonderdeel en stuurt op beveiligingsbewustzijn en naleving van regels en richtlijnen zoals die zijn vastgelegd in planningsgesprekken of procedures. Het management laat hier in voorbeeld gedrag zien. Informatiebeveiliging is periodiek een onderwerp van gesprek in overleggen wanneer binnen afdelingen en bureaus met bedrijfskritische of anderszins gevoelige informatie wordt gewerkt. Managers dragen zorg voor continue opleiding en bijscholing rond het gebruik van informatiesystemen en informatieveiligheid voor medewerkers binnen zijn of haar organisatieonderdeel. Deze zorg heeft de vorm van het met de medewerker definiëren van de benodigde opleidingen, het gelegenheid geven tot het volgen er van en het bespreken van het opleidingsresultaat. Het management is verantwoordelijk voor het nemen van besluiten over informatiebeveiligingsmaatregelen, waarbij afgestemd wordt met intern verantwoordelijken. Dit geldt ook voor het aangaan, wijzigen en beëindigen van een dienstverband of overeenkomst. De besluiten worden structureel door het management geëvalueerd, mede op basis van toetsing en rapportage door de CISO, FG en Archiefinspecteur.

3. Het **College** is bestuurlijk verantwoordelijk voor informatiebeveiliging en privacybescherming en stelt hiervoor kaders vast. Ze wordt hierin geadviseerd door de gemeentesecretaris, die op zijn/haar beurt geadviseerd wordt door Bureau Ontwikkeling I&A / CIO en Stadscontrol / CISO-FG (waarbij de CISO-FG het College zelfstandig en "bindend"[4] kan adviseren). De kaders worden structureel door het College geëvalueerd en bijgesteld waar nodig. Het College stelt kaders voor informatiebeveiliging publiek beschikbaar en communiceert richting betrokkenen en de gemeenteraad over de wijze waarop ze de kaders uitvoert, op basis van de toetsing en rapportage door Stadscontrol / CISO-FG. De gemeentelijke rekenkamer kan besluiten hierop toe te zien.

4. **Concernmanager** - Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Nijmegen (gegevensverwerkingen) hebben een interne verantwoordelijke ("eigenaar") die de waarde bepaalt van de informatie die ze bevatten. Dit geldt ook voor generieke systemen zoals mail. Voor al deze " bedrijfsmiddelen" is deze eigenaar ook vastgelegd. De primaire verantwoordelijkheid binnen de gemeente Nijmegen voor de bescherming van informatie ligt bij deze eigenaar van de informatie. De verantwoordelijkheid voor specifieke beheersmaatregelen mag worden gedelegeerd, worden toegekend aan een medewerker in de vorm van een rol of taak (met de benodigde autorisaties), maar de eigenaar blijft verantwoordelijk voor een goede bescherming. De eigenaar is altijd een concernmanager. Bij extern beheerde informatiebronnen en –systemen heeft de eigenaar de rol van opdrachtgever. De intern verantwoordelijke ziet er op toe dat het informatiebeveiligingsbeleid en de deelaspecten ervan, zoals het beleid op ICT-bedrijfscontinuïteit en privacybescherming, wordt uitgevoerd (meestal in de vorm van beheersmaatregelen) voor de informatiebronnen en –systemen waar deze verantwoordelijk voor is.

[4] Door het advies ook rechtstreeks (buiten de gemeentesecretaris en College om) aan de Autoriteit Persoonsgegevens te sturen, die hierop kan besluiten in te grijpen.

5. **CIO** – De Chief Information Officer (CIO) is op strategisch niveau verantwoordelijk voor het beveiligen van de informatie om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is om de bedrijfscontinuïteit, het behalen van maatschappelijke doelen te kunnen waarborgen. De CIO wordt op gebied van informatiebeveiliging vervangen door de Security Officer (SO). De CIO escaleert in besluitvorming naar de Stadscontroller, de Gemeentesecretaris en wanneer openbare orde in het geding is, naar de Burgemeester.

6. **Adviseur** - Het management wordt daarnaast geadviseerd bij het nemen van besluiten en kan het nemen van besluiten binnen bestaand beleid mandateren aan de adviserende rollen, mits in samenspraak met betrokken intern verantwoordelijken:
    a. ICT-maatregelen/-aspecten: Bureau Ontwikkeling I&A / CIO
    b. Facilitaire en huisvestingsmaatregelen/-aspecten: Bureau Facilitaire Zaken
    c. Maatregelen op gebied van documentbeheer en archivering/-aspecten: Bureau Documentaire Informatievoorziening
    d. Inkoop- en financiële maatregelen/-aspecten: Afdeling Financiën
    e. Personele en organisatorische maatregelen/-aspecten: Bureau P&O Beleid/Advies en de Ondernemingsraad
    f. Procesinhoudelijke maatregelen/-aspecten: Afdelingshoofden betrokken afdelingen
    g. Juridische maatregelen/-aspecten: Afdeling Juridische Zaken

7. **Beheerder** - Het realiseren en uitvoeren van informatiebeveiligingsmaatregelen is een gedeelde verantwoordelijkheid, waarbij besluiten zoals hierboven beschreven leidend zijn. Wel zijn een aantal specifieke partijen verantwoordelijk voor een deel van de realisatie en (continue) uitvoering van maatregelen. Waar uitvoering van maatregelen meerdere verantwoordelijkheden raken, wordt in de uitvoering samengewerkt en deelverantwoordelijkheden afgestemd:
    a. ICT-maatregelen: Bureau Ontwikkeling I&A / CIO (ontwerp, architectuurbewaking en ontwikkeling), ICT-bedrijf Rijk van Nijmegen (functioneel beheer alle applicaties en systemen t.b.v. gemeente Nijmegen), Bureau basisregistraties en gegevensmanagement (beheer en levering (geo-)informatie), Bureau financiële administratie (beheer financiële systemen), Bureau P&O services (beheer personele systemen), Afdeling VSA (ICT-componenten beheer accommodaties), afdeling Stadsbeheer (ICT-componenten beheer openbaar ruimte en ondergrondse ICT-infrastructuur)
    b. Facilitaire en huisvestingsmaatregelen: Bureau Facilitaire Zaken, Afdeling Vastgoed en Sport Accommodaties
    c. Maatregelen op gebied van documentbeheer en archivering: Bureau Documentaire Informatievoorziening, Regionaal Archief Nijmegen (RAN)
    d. Inkoop- en financiële maatregelen: Afdeling Financiën
    e. Personele en organisatorische maatregelen: Bureau P&O Services
    f. Procesinhoudelijke maatregelen: Afdelingshoofden betrokken afdelingen
    g. Juridische maatregelen: Afdeling Juridische Zaken

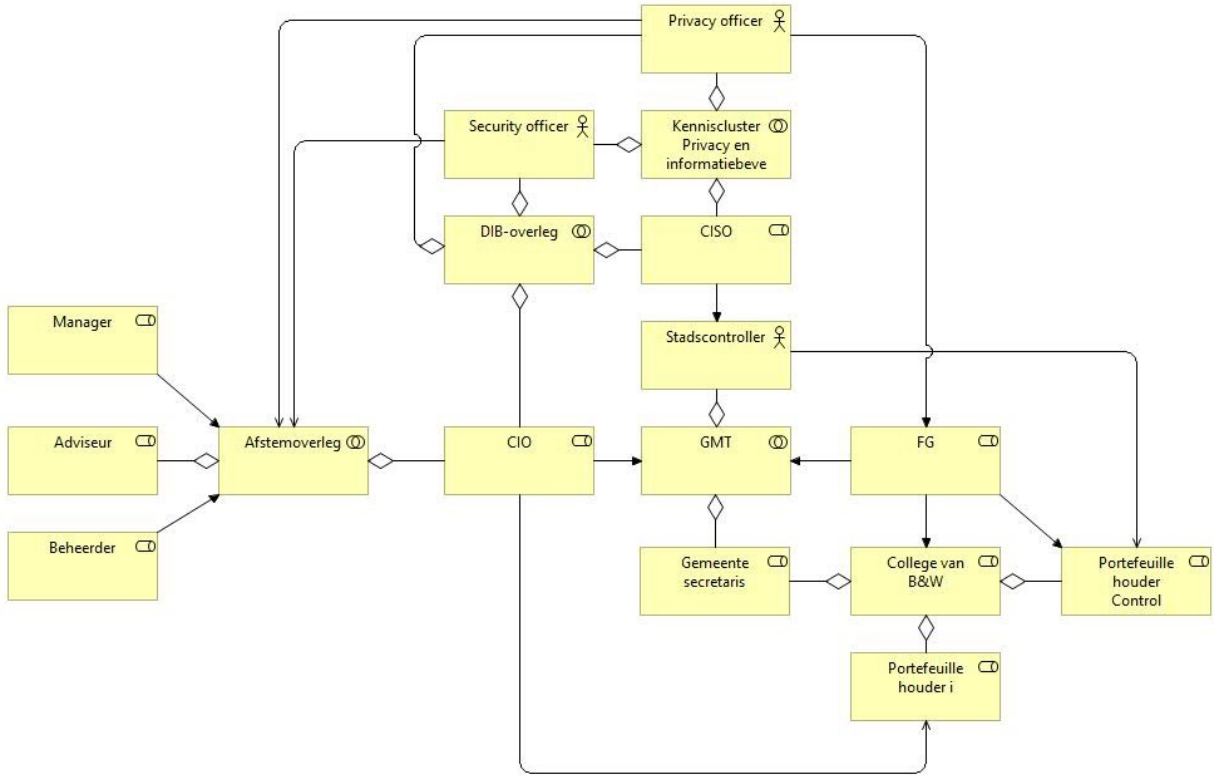
8. De **CISO**, **FG** en **Archiefinspecteur** zijn strategisch verantwoordelijk voor het houden van onafhankelijk toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met informatie, waaronder persoonsgegevens. De Chief Information Security Officer (CISO) is op strategisch niveau verantwoordelijk voor het beveiligen van de informatie om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is om de bedrijfscontinuïteit, het behalen van maatschappelijke doelen te kunnen waarborgen. De CISO is verantwoordelijk voor het coördineren van informatiebeveiligingsincidenten: het analyseren van het incident, het adviseren over en het coördineren van te nemen maatregelen om incidenten op te lossen, de gevolgen ervan te beperken en het voorkomen van herhaling ervan. De CISO wordt vervangen door de Security Officer (SO) of de Privacy Officer (PO). De FG is strategisch verantwoordelijk voor de bescherming van de privacy van burgers en medewerkers van gemeente Nijmegen en zorgt voor het toezicht op de uitvoering van het privacy beleid. De FG wordt vervangen (tijdelijk) door de PO. De Archiefinspecteur adviseert en controleert de eigenaar en de beheerder bij de bescherming van archiefwaardige informatie. Deze rol wordt ingevuld door twee medewerkers.
   De advies- en toezichtsrol van de CISO, FG en Archiefinspecteur is erop gericht dat de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen, om zo risico's te beheersen. Ten behoeve van het toezicht wordt er

getoetst, onder andere op KPI`s die ontwikkeld worden in samenwerking met de iRvN. De CISO, FG en Archiefinspecteur rapporteren hierover richting het management en het College. In het uitvoeren van de advies- en toezichtsrol wordt samengewerkt met andere hier genoemde partijen. De CISO, FG en Archiefinspecteur escaleren in besluitvorming naar de Stadscontroller, de Gemeentesecretaris en wanneer openbare orde in het geding is, naar de Burgemeester.

9. De **Securityofficer** (SO) en **Privacyofficer** (PO) hebben een adviserende en tactisch-ondersteunende rol op het gebied van informatiebeveiliging (SO) en privacybescherming (PO). De SO adviseert het afdelingshoofd, de CISO en CIO in het beveiligen van de informatie van de gemeente om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is voor de dienstverlening. De SO escaleert in besluitvorming naar de CISO of CIO. De PO adviseert de FG bij de bescherming van de privacy van burgers en medewerkers van gemeente Nijmegen. De PO escaleert in besluitvorming naar de FG (functioneel) of een manager.

   Daarnaast zijn er deelfuncties die controle en rapportagetaken uitvoeren op specifieke deelgebieden:
   a. SUWI/Suwinet: coördinator kwaliteitsbeheer afdeling Zorg en Inkomen
   b. BRP: beveiligingsbeheerder BRP
   c. Reisdocumenten: beveiligingsfunctionaris reisdocumenten
   d. Rijbewijzen: beveiligingsfunctionaris rijbewijzen

10. Waar verantwoordelijkheden, domeinen en deelaspecten van informatiebeveiliging elkaar raken wordt er **samengewerkt**. Regulier bestaan er samenwerkingen op gebied van:
    a. Het GMT met leden van de Directie en de CIO als deelnemers. In deze samenwerking worden kaders en besluiten op gebied van informatiebeveiligingsbeleid voorbereid en besluiten genomen op gebied van informatiebeveiligingsmaatregelen voor de gemeentesecretaris en College.
    b. De werkgroep DIB (Digitaal Informatiebeleid) met als voorzitter de CIO. In deze samenwerking worden kaders en besluiten op gebied van informatiebeveiligingsbeleid voorbereid voor het GMT. De SO en PO nemen deel aan deze werkgroep wanneer informatiebeveiligingsbeleid en/of privacybeleid op de agenda staan.
    c. Het afstemmingsoverleg met als voorzitter de CIO. In deze samenwerking worden besluiten genomen op gebied van informatiebeveiligingsmaatregelen en besluiten voorbereid met een hoge impact, voor het GMT. De adviseurs onderzoeken en verkennen vernieuwingen met ICT-aspecten (intake) en betrekken de SO en/of de PO wanneer informatiebeveiliging of privacy mogelijk geraakt worden. De adviezen van de SO en/of de PO worden vastgelegd bij de intakes.
    d. Het kenniscluster privacy en informatiebeveiliging, waar privacyjuristen, de SO/i-adviseur, CISO en de PO (voorzitter) (FG als toehoorder) aan deelnemen. In deze samenwerking worden juridische kaders en beleid op gebied van privacy en informatiebeveiliging voorbereid en afspraken gemaakt over de uitvoering van maatregelen op gebied van privacy en informatiebeveiliging.
    e. In het geval van een ICT crisis wordt op gemeentelijk crisisteam opgeroepen door de gemeentesecretaris. Dit orgaan bestaat uit:
       - Gemeentesecretaris (voorzitter)
       - Afdelingshoofd PIF
       - Afdelingshoofd Stadscontrol
       - CIO
       - CISO
       - Afdelingshoofd van de afdeling die geraakt is door de crisis



Figuur 2: samenwerkingen

Welke maatregelen kennen wij m.b.t. externe partijen?

- De iRvN (ICT Rijk van Nijmegen) is onderdeel van een gemeenschappelijke regeling waar de gemeente Nijmegen aan deelneemt en heeft een belangrijke rol in het realiseren van de doelstellingen in het informatiebeveiligingsbeleid. De iRvN voert ICT-(beveiligings)maatregelen uit voor de gemeente Nijmegen en andere regionale gemeenten en is eigenaar van een regionale ICT-infrastructuur. Met de iRvN is een dienstverleningsovereenkomst gesloten, waarvoor de CIO regie heeft. De iRvN coördineert de levering en beheer van ICT-hardware en mobiele devices, binnen de kaders van het informatiebeveiligingsbeleid. De iRvN en daarmee haar medewerkers heeft voor de gemeente Nijmegen over het algemeen de rol van beheerder.
- Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).5 Voor externe partijen geldt hierbij het “pas toe of leg uit” beginsel alleen nog waar de BIO niet van toepassing is.
- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV) en de ICT Inkoopvoorwaarden (GIBIT), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV dienen te worden getoetst aan Informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of verwerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.6
- Om op de uitvoering van afspraken te kunnen sturen en toetsen worden KPI`s en toetsingsmethoden ontwikkeld.
- Voor het tot stand brengen van datakoppelingen met externe partijen, gelden naast dit generiek informatiebeveiligingsbeleid specifieke procedures. Het doel van deze procedures is risicobeheersing.

[5] Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.
[6] Hiervoor kan gebruik worden gemaakt van een ‘third party mededeling’ (TPM), ISO27001 of een ISAE 3402-verklaring.

- Voor externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing7 zoals die geformuleerd worden in de Cloud Security Alliance Controls Matrix van de Cloud Security Alliance. Ook in deze gevallen blijft de gemeente verantwoordelijk voor de betrouwbaarheid van de uitbestede diensten.
- De gemeente is gehouden aan:
    - regels omtrent communicatie met externe partijen (zoals rond veilig mailen)
    - regels omtrent grensoverschrijdend dataverkeer;
    - toezicht op naleving van regels door externe partijen;
    - waarborgen van rechten van betrokkenen;
    - hoogste beveiligingseisen voor bijzondere categorieën gegevens;8
    - melding bij de Autoriteit Persoonsgegevens bij uitbesteding van het bewerken van persoonsgegevens en toestemming van de Autoriteit Persoonsgegevens bij doorgifte van persoonsgegevens naar landen buiten de EU.

Welke maatregelen kennen wij m.b.t. ICT crisisbeheersing?

- Voor interne crisisbeheersing kan er een crisisteam worden geformeerd op initiatief van de CISO/FG. Dit team is aangesloten op de structuren zoals die gebruikt worden in de rampenbestrijding. De werkwijze dient te zijn vastgelegd en geoefend. In de Rapportage Procesbeschrijving 1.1 is beschreven wat het proces is bij het bestrijden van een ICT crisis. Daarin speelt ook de koppeling met de regio en belangrijke rol. Het Crisisteam oefent een keer per jaar een crisis, waarbij de oefening ook geëvalueerd wordt. Daarnaast worden periodiek casussen besproken uit de praktijk.

Welke maatregelen kennen wij m.b.t. Suwinet

- De Security Officer
- Adviseert en rapporteert periodiek richting Directeur op het gebied van gebruik- en informatiebeveiliging Suwinet ;
  Controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd;
  Rapporteert beveiligingsincidenten richting verantwoordelijk afdelingshoofd en ziet toe op passende vervolgactie;
- Voert periodieke controles uit op een rechtmatig gebruik van Suwinet-inkijk;
  Doet voorstellen tot implementatie of aanpassing van plannen en werkprocessen op het gebied van de beveiliging;
  Houdt toezicht op het feit dat nieuwe medewerkers (ook extern personeel) worden
  geïntroduceerd en bekend gemaakt met de beveiligingsprocedures;
  Fungeert als centraal aanspreekpunt op het gebied van beveiliging Suwinet;
- De gebruikersbeheerder
- Voert beheersmatige werkzaamheden uit met betrekking tot locatie(s), systemen, gegevens en bedrijfsvoering
- Adviseert op het gebied van gegevensbeheer en documentaire informatievoorziening
- Beheert, controleert en onderhoudt gegevens en informatie voor meerdere samenhangende werkterreinen
- Het beveiligingsbeleid/plan is aantoonbaar centraal beschikbaar voor alle gebruikers op iNsite, de interne internetpagina
- Medewerkers zijn via iNsite middels het beschikbaar stellen van Beveiligingsplan op de hoogte gebracht van het bestaan, aard en doel van de logging van Suwi-raadplegingen en dat oneigenlijk gebruik sancties tot gevolg heeft (zie ook ‘Procedure controle gebruik Suwinet-Inkijk - Controleplan’)
- Toewijzen autorisaties:
  Het gebruik van Suwinet-Inkijk is voorbehouden aan de medewerkers van de afdeling Zorg en Inkomen. De autorisaties voor Suwinet-Inkijk worden in beginsel per functiegroep toegekend.
  De security officer bepaalt welke autorisaties een medewerker toegekend krijgt voor het uitvoeren van zijn of haar taken. De wijze waarop de autorisaties worden toebedeeld, gewijzigd of ingetrokken is nader vastgelegd in de bijlage

---

7 Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
8 Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen

'Procedure autorisaties'.
De medewerkers die een autorisatie voor Suwinet-Inkijk aanvragen, doen dat middels een webformulier. Daarbij moet de medewerker tevens een zorgvuldigheidsverklaring ondertekenen.
Dit geldt ook voor extern personeel.

- Functiescheiding:
  Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor Suwinet. Het gaat dan met name over functiescheiding. Zo zijn de functies gebruik van Suwinet, beheer van autorisaties Suwinet, controle op het gebruik van Suwinet en beslissen over wie welke functies krijgt in Suwinet gescheiden. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt. De diverse functies noodzakelijk voor Suwinet en de overweging voor het toebedelen van de taken, profielen en rollen zijn schriftelijk vastgelegd, Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken.
  - uitvoering van taken (raadpleegfunctie Suwinet) ligt bij de reguliere gebruikers zoals klantmanagers, inkomensconsulenten en medewerkers Handhaving
  - beheer van autorisaties en toegang verlenen tot Suwinet ligt bij enkele medewerkers van de ICT-afdeling (IRvN)
  - kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, namens de security officer Suwinet) ligt bij kwaliteitsmedewerkers Zorg en Inkomen.
  - management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet) ligt bij de Security Officer (namens gemeentesecretaris en College).

Welke maatregelen kennen wij m.b.t. reisdocumenten/rijbewijzen

- De wetgever stelt eisen aan de opslag, uitgifte en administratie van reisdocumenten. Voor reisdocumenten zijn deze eisen neergelegd in artikel 90 van de Paspoortuitvoeringsregeling Nederland 2001, (PUN). "De met de uitvoering van de wet belaste autoriteiten treffen maatregelen om de onder hen berustende reisdocumenten, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreem-ding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins".

- De beveiligingsfunctionaris reisdocumenten/rijbewijzen is door de burgemeester aangewezen en is belast is met het beheer van en het toezicht op de naleving van de beveiligingsprocedure. Van de aanwijzing of de vervanging van de beveiligingsfunctionaris reisdocumenten wordt direct schriftelijk melding gedaan aan de Rijksdienst voor Identiteitsgegevens (RvIG).

- *Taken en verantwoordelijkheden van de beveiligingsfunctionaris*: Wordt bij het definitief invullen van de vragenlijst (kwaliteitsmonitor en Ensia) betrokken door Publiekszaken; Neemt deel aan het veiligheidsoverleg; Controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd; Rapporteert beveiligingsincidenten richting verantwoordelijk afdelingshoofd en ziet toe op passende vervolgactie; Doet voorstellen tot implementatie of aanpassing van plannen en werkprocessen op het gebied van de beveiliging; Houdt toezicht op het feit dat (nieuwe) medewerkers (ook extern personeel) ten minste één maal per jaar worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures; Fungeert als centraal aanspreekpunt op het gebied van beveiliging;

- Om de kans te verkleinen dat medewerkers Publiekszaken door kwaadwillenden worden misleid (externe fraude), of dat zij al dan niet onder druk van chantage, bedreiging of omkoping misbruik maken van hun bevoegdheden (interne fraude), is functiescheiding bij het verstrekken van waarde documenten noodzakelijk. Op grond van art. 93 van de PUN wordt functiescheiding toegepast:

    - Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende- en beheertaken met betrekking tot reisdocumenten;

- Tussen aanvraag/verstrekking, beheer en uitreiking van reisdocumenten. Indien door een te geringe personele capaciteit laatstgenoemde functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Zoals opgenomen in de procedure ontbreken van voldoende functiescheiding.

Welke maatregelen kennen wij m.b.t. de BRP

- Functiescheiding: Zo zijn de functies gebruik van de BRP, beheer van autorisaties BRP, controle op het gebruik van de BRP en beslissen over wie welke profielen krijgt in de BRP gescheiden. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt. De diverse functies noodzakelijk voor de BRP en de overweging voor het toebedelen van de taken, profielen en rollen zijn schriftelijk vastgelegd, Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken o.a. weergegeven in de:
  - De Regeling beheer en toezicht BRP gemeente Nijmegen 2022;
  - De uitvoeringsregeling BRP;
  - Het Reglement BRP;
- De Regeling bestuurlijke boete.

7. Beheer van bedrijfsmiddelen – maatregelen met betrekking tot informatie

Wie is verantwoordelijk voor de bedrijfsmiddelen?

- Alle bedrijfsmiddelen moeten geïdentificeerd zijn en er moet een inventaris van worden bijgehouden.
- Regels vaststellen, documenteren en implementeren voor het aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- Privégebruik van informatie en bestanden is niet toegestaan. Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld in het Thuiswerkbeleid.
- De medewerker zelf neemt passende technische en organisatorische maatregelen om informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
  - de beveiligingsclassificatie van de informatie (zie hieronder);
  - de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid);
  - aan de werkplek verbonden risico's;
  - Het risico door het benaderen van informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

Hoe classificeren wij informatie?

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt.9 Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid (= BIV). De classificatie van de informatie is onderdeel van de uit te voeren DPIA, die ook eigenaarschap en andere randvoorwaarden vastlegt.

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

[9] Dit is in detail beschreven in de component architectuur Informatiebeveiliging 2014, CIO, 2014.

Welke maatregelen naar aanleiding van classificatie informatie?

- De eigenaar van de gegevens is de proceseigenaar. De eigenaar van de gegevens bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen, wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt wie toegang krijgt tot welke gegevens en met welke rechten. Voor classificatie wordt hierbij uitgegaan van collectieve eigenaarschap van het College.
- De classificatie heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten. In de BIO omvat het begrip informatiesysteem alle genoemde elementen.
- Het object van classificatie is informatie. We classificeren op het niveau van informatiesystemen (of informatieservices). Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de CISO/SO in het ISMS en dienen jaarlijks gecontroleerd te worden door de eigenaren.
- De eigenaar van de gegevens (intern verantwoordelijke) bepaalt het vereiste beschermingsniveau (classificatie), waarbij afgestemd wordt met alle betrokkenen.
- Er wordt gestreefd naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid). De door de VNG gehanteerde referentiecomponenten (GEMMA2) en hun classificatie zijn hier relevant.
  Per classificatieniveau en aspect is bepaald welke beveiligingsmaatregelen genomen dienen te zijn. Er wordt gestreefd naar een balans tussen het te lopen risico en de kosten van tegenmaatregelen. Een technische oplossing verdient altijd de voorkeur boven gedragsverandering of een administratieve procedure.
- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Aanvullende veronderstellingen worden alleen geformuleerd bij classificaties "geen", midden (M) en hoog (H). Afwijkingen moeten worden aangegeven.
- Interne bedrijfsvoering, externe dienstverlening en (keten-) samenwerking zijn voor het classificeren van gelijk belang.
- Classificatie geldt voor de gemiddelde situatie.
- De geclassificeerde waarde van informatie is een basis voor het nemen van beslissingen over ICT binnen de gemeente en wordt als zodanig uitgedragen. Classificatie is opgenomen in de procedure voor het ontwikkelen of verwerven van nieuwe informatiesystemen en -bronnen.

Niveau / impact	Beschikbaarheid (B)	Integriteit (I)	Vertrouwelijkheid (V)	Duurzaamheid
Geen	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn.	**Niet zeker, geen** informatie mag worden veranderd	**Openbaar** informatie mag door iedereen worden ingezien. Informatie is rechtenvrij (open data).	**Standaard** Geen duurzaam informatiebeheer noodzakelijk (Gegevens zijn na invoeren binnen 10 jaar niet meer relevant)
Laag	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn. Maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen. Uitval is niet meteen productieverstorend, er zijn work-arounds mogelijk: - financiële gevolgen makkelijk op te vangen; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade).	**Beschermd** het bedrijfsproces en wetgeving staan enkele (integriteits-) fouten toe. Onjuistheid gegevens valt op of heeft weinig impact: - financiële gevolgen makkelijk op te vangen; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade).	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie. Informatie is niet rechtenvrij, maar bevat geen (privacy-)gevoelige informatie die afscherming vraagt. Impact van doorbreken: - financiële gevolgen makkelijk op te vangen; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade).	

Niveau / impact	Beschikbaarheid (B)	Integriteit (I)	Vertrouwelijkheid (V)	Duurzaamheid
Midden	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk. Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur). Uitval beschikbaarheid is productieverstorend, maar heeft geen directe externe impact: - bestuurder moet zich verantwoorden; - schade te herstellen door ambtelijke opschaling; - financiële gevolgen niet meer op te vangen binnen de vastgestelde begroting - geen accountantsverklaring; - organisatiebrede negatieve publiciteit (imagoschade); - significant verlies van motivatie van medewerkers.	**Hoog** het bedrijfsproces en wetgeving staan zeer weinig fouten toe. Onjuistheid gegevens valt niet snel op en/of kan leiden tot problemen: - bestuurder moet zich verantwoorden; - schade te herstellen door ambtelijke opschaling; - financiële gevolgen niet meer op te vangen binnen de vastgestelde begroting	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers. Informatie mag alleen geraadpleegd worden als het noodzakelijk is voor rol/functie. Impact van doorbreken: - bestuurder moet zich verantwoorden; - schade te herstellen door ambtelijke opschaling; - financiële gevolgen niet meer op te vangen binnen de vastgestelde begroting	**Hoog** Duurzaam informatiebeheer noodzakelijk (Gegevens zijn na invoeren na 10 jaar of meer nog relevant)
Hoog	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten. Uitval beschikbaarheid heeft een directe en hoge impact: - politieke schade aan een bewindspersoon/college; - financiële schade meer dan 2% van het gemeentebudget; - een jaar vertraging van nieuwe ontwikkelingen - negatieve publiciteit op landelijk niveau (imagoschade) - ernstige afname van personele capaciteit.	**Absoluut** het bedrijfsproces en wetgeving staan geen fouten toe. Onjuistheid gegevens heeft altijd impact: Zware maatschappelijke schade; - grote impact voor betrokkene(n); - onmogelijk om de gegevens te herstellen; - volledig stilvallen van een kritisch proces;	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n). Informatie mag alleen geraadpleegd worden als het noodzakelijk is voor rol/functie en er een directe betrokkenheid op persoonsniveau is.	

Hoe wordt bepaald wat passend is?

De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie-afhankelijk, daarom kan een classificatie voor buiten kantooruren, op betaaldagen, afwijken. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd, dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien

de kosten voor het beperken van de risico's disproportioneel hoog zijn.[10] Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

In de komende paar jaar zullen de systeem eigenaren (over het algemeen concernmanagers) door middel van business impact analyse vragenlijsten de classificatie van hun systemen controleren en door middel van hun risicoafweging bepalen welke maatregelen nog genomen worden. Voor niet toegewezen gegevensverzamelingen is de gemeente secretaris verantwoordelijk.

8. Beveiliging van personeel – maatregelen in het personeelsbeleid

Welke maatregelen worden getroffen mbt personeel

- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van de proceseigenaar van het desbetreffende bedrijfsproces ingetrokken.
- Er wordt naar gestreefd om medewerkers die werken met vertrouwelijke of geheime informatie voor indiensttreding een Verklaring Omtrent het Gedrag (= VOG) te laten overleggen. De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Het vergroten van het bewustzijn van informatiebeveiliging is onderdeel van het permanente opleidingsprogramma dat in verschillende vormen aan de medewerkers wordt aangeboden. Het opleidingsprogramma is een van de speerpunten van het leren en ontwikkelen systeem dat door P&O wordt vormgegeven. Zie hier voor het P&O beleid op dit terrein.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en regelingen.
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

9. Fysieke beveiliging en beveiliging van de omgeving – beveiliging van gebouwen

Welke maatregelen kennen we voor gebouwen?

- Alle objecten (gebouwen) van de gemeente krijgen op basis van generieke profielen een risicoprofiel toegewezen. Dit is het generieke risicoprofiel dat het beste aansluit bij het object.
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- In diverse panden van de gemeente wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is beperkt door de Algemene Verordening Gegevensbescherming (AVG) en nadere regels.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende 'best practices'.
- (Data)verbindingen worden beschermd tegen interceptie of beschadiging.
- Reserve apparatuur en back-ups zijn gescheiden in twee locaties of datacenters, om de gevolgen van een calamiteit te minimaliseren.

[10] Dit is uitgebreid beschreven in: 'Beveiliging van persoonsgegevens', AUTORITEIT PERSOONSGEGEVENS richtsnoeren, 2013.

- Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten.

10. Beheer van communicatie en bedieningsprocessen – maatregelen mbt beheer van IT systemen.

Welke maatregelen kennen we mbt de organisatie van beheer?

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Externe hosting van data en/of services wordt:
  - goedgekeurd door intern verantwoordelijke (“eigenaar”);
  - geregeld in overeenstemming met het informatiebeveiligingsbeleid (getoetst door CISO/FG);
  - vooraf gemeld bij de afdeling Personeel Informatie en Facilitair t.b.v. toetsing op beheeraspecten.

Welke maatregelen zijn er m.b.t. systeemplanning en –acceptatie?

- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
- Systemen voor Test (T) en/of Acceptatie (A) zijn logisch gescheiden van Productie (P).
- Faciliteiten voor testen, acceptatie en productie zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de test en acceptatie omgeving worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
- Vertrouwelijke of geheime data uit de productieomgeving mag niet worden gebruikt in de test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data op dezelfde wijze te beschermen als productie data.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Welke maatregelen zijn er m.b.t. versleuteling?

- De gemeente gebruikt encryptie conform PKI-overheid standaard.[11]
- Versleuteling vindt plaats conform ‘best practices’ (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- Intern dataverkeer (‘machine to machine’) wordt conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden centraal beheerd.

Welke maatregelen zijn er op het vlak van ons netwerk?

- Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.
- Het netwerk is waar mogelijk gesegmenteerd (organisatie onderdelen, gebruikers en systemen zijn logisch gescheiden). Tussen segmenten met verschillende beschermingsniveaus worden access control lists (ACL’s) geïmplementeerd.

[11] Public Key Infrastructure voor de overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.

- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.
- Alle apparatuur die is verbonden met het netwerk van de gemeente moet kunnen worden geïdentificeerd.

Welke maatregelen nemen we m.b.t. het beheer van mobiel werken?

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software'). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van informatie en integriteit van het netwerk. Dit verzoek is nog niet gedaan.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen mogelijk betrekking hebben op privémiddelen en privébestanden. Hiervoor wordt een regeling ontwikkeld.

Welke maatregelen nemen we als het gaat om back-up en recovery?

- In opdracht van de eigenaar van data, maakt de afdeling iRvN reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
- Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen.
- De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

Welke maatregelen nemen we als het gaat om informatie-uitwisseling

- Voor het gebruik van informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, geheimhoudingsverklaring, huisregels.
- Digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld.
- Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.
- Informatie-uitwisseling voldoet aan standaarden zoals beschreven door het forum standaardisatie, waaronder in ieder geval:
    - DNSSEC: Domeinnaambeveiliging
    - TLS: Beveiligde verbinding
    - DKIM: Anti-Phishing
    - SPF: Anti-Phishing
    - DMARC: Anti-Phishing
- Met betrekking tot het uitwisselen van informatie via social media staan de overwegingen voor de keuze van het kanaal uitgewerkt in het document Keuze en Gebruik Dienstverleningskanalen.

Welke maatregelen gelden bij het ontwikkelen en onderhouden van software?

- Applicaties worden door derden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties.[12] Er wordt ten minste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10 voor webapplicaties.[13]
- Web applicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).

[12] Nationaal Cyber Security Centrum, NCSC
[13] https://www.owasp.org/index.php/Main_Page

- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door checksums).
- Alleen gegevens die noodzakelijk zijn voor de taak worden verzameld en beheerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
- Technische kwetsbaarheden worden regulier met een minimum van 12 keer per jaar gerepareerd door 'patchen' van software, of 'ad hoc' bij acute dreiging. Welke software wordt geüpdatet wordt bepaald door de risico's.

Welke maatregelen worden getroffen m.b.t. logging en audit trail?

- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.[14]
- Relevante zaken om te loggen zijn:
  - type gebeurtenis (zoals back-up/restore, reset van een wachtwoord, betreden ruimte);
  - handelingen met speciale bevoegdheden;
  - (poging tot) ongeautoriseerde toegang;
  - systeemwaarschuwingen;
  - (poging tot) wijziging van de beveiligingsinstellingen.
- Een logregel bevat minimaal:
  - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
  - de gebeurtenis;
  - waar mogelijk de identiteit van het werkstation of de locatie;
  - het object waarop de handeling werd uitgevoerd;
  - het resultaat van de handeling;
  - de datum en het tijdstip van de gebeurtenis.
- In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
- Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of de systeembeheerder. De bewaartermijnen zijn in overeenstemming met wettelijke eisen zoals de archiefwet.
- De doelstellingen voor logging, de aansluiting op het EWS/SIEM en wat er gelogd wordt van welke applicaties wordt beschreven in het logging beleid.

Welke technische beheersmaatregelen zijn er nog meer?

- Alle gegevens anders dan classificatie 'geen' worden beveiligd conform beveiligingseisen in de IB-architectuur. Classificatieniveau 'laag': transportbeveiliging buiten het interne netwerk; Classificatieniveau 'midden': transportbeveiliging; Classificatieniveau 'hoog': transport en berichtbeveiliging.
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.
- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software van verschillende leveranciers toegepast.
- 'Mobile code'[15] wordt uitgevoerd in een logisch geïsoleerde omgeving om de kans op aantasting van de integriteit van het systeem te verkleinen. De 'mobile code' wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van 'geheime' gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.

[14] In sommige processen is het wettelijk verplicht of zeer gewenst dat geautoriseerde toegang wordt vastgelegd, zodat achteraf steeds kan worden vastgesteld wie toegang tot de gegevens heeft gehad.

[15] Software die wordt uitgevoerd zonder expliciete toestemming van de gebruiker, zoals scripts (Java), Java applets, ActiveX controls en Flash animaties. Dergelijke software wordt gebruikt voor functies binnen (web)applicaties.

- Het automatisch doorsturen van e-mails is niet toegestaan.
- Alle informatie, die wordt geplaatst op websites van de gemeente, wordt beschermd tegen onbevoegde wijziging. Op algemeen toegankelijke websites wordt alleen openbare informatie gepubliceerd.
- Groepen informatiediensten, gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind.
- Afhankelijk van de risico's die verbonden zijn aan online transacties worden maatregelen getroffen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging, openbaarmaking, duplicatie of weergave te voorkomen.

Welke risico's zijn er als de dienstverlening door een derde wordt beheerd?

Ingeval de gemeente diensten heeft uitbesteed, is er volgens de baseline sprake van een specifieke set aan te beperken risico's in dit domein:

- De gemeente gaat steeds meer samenwerken en informatie uitwisselen in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij kan ook informatie van de gemeente op straat komen te liggen.
- De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in de keten, ook al is het beheer bij een andere partij neergelegd.

Welke IB doelen streven wij na bij dienstverlening door een derde?

- Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (bewerkers)overeenkomst, contracten en/of convenanten.
- De organisatie controleert de implementatie van de maatregelen, die zijn vastgelegd in overeenkomsten, bewaakt de naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de beveiliging aan alle eisen voldoet, die met de derde partij zijn overeengekomen.

Welke maatregelen treffen wij als de dienstverlening door een derde wordt beheerd?

- Implementatie en uitvoering van de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door de derde partij.
- Controle en beoordeling van de diensten, rapporten en registraties, die door de derde partij worden geleverd.
- Er worden periodiek audits uitgevoerd. Er worden KPI`s ontwikkeld om sturing te verbeteren.
- Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging worden altijd afgestemd door de in de overeenkomsten benoemde contactpersonen.
- In de met de derde partij overeengekomen SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging. Hiervoor wordt veelal verwezen naar de ICT Inkoopvoorwaarden en een eventueel aanwezige bewerkersovereenkomst.
- In de met de derde partij afgesloten overeenkomsten wordt beschreven hoe de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) geregeld is door kaders aan te geven voor de toegang tot ICT-voorzieningen. In contractbeheer, applicatiebeheer en functioneel beheer is controle op naleving van de gemaakte afspraken opgenomen.

Daarnaast heeft de gemeente Nijmegen een aantal specifieke kwaliteitseisen ten aanzien van ICT-dienstverlening door derden. Deze worden waar relevant benoemd in het programma van eisen.

- De derde partij voorkomt dat gedeelde componenten met andere klanten in de infrastructuur de performance bedreigen.
- De derde partij voorkomt dat het gedrag van andere klanten de performance van de diensten van Opdrachtgever bedreigd.
- De derde partij zorgt ervoor dat Opdrachtgever is beschermd tegen het gedrag van andere klanten. (bijv. spamming vanuit eenzelfde ipadres).
- De derde partij zorgt voor afdoende isolatie in de virtualisatie en storage-lagen.
- De derde partij zorgt er voor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door partijen die actief zijn binnen het leverancier netwerk.
- De derde partij voorkomt dat inbeslagname van voor de klant kritieke netwerkcomponenten door een dwangbevel gericht op een andere klant voor Opdrachtgever gevolgen hebben.
- De derde partij beschrijft hoe wordt omgegaan met verzoeken tot het blokkeren van klantomgevingen of het overhandigen van klantdata.

- De derde partij beschrijft, ook voor personeel, waar sprake kan zijn van conflicterende rollen en hoe daar mee omgegaan wordt.
- De derde partij beschrijft hoe beschikbaarheids-risico's worden beperkt via o.a. een beschrijving van de redundantie in verschillende componenten in de netwerk, server en opslag-lagen.
- De derde partij beschrijft hoe performance-aspecten van de diensten worden beheerd via o.a. een beschrijving van de netwerk snelheid, CPU en opslagcapaciteit.
- De derde partij beschrijft hoe wordt omgegaan met crisissituaties o.a. via welke uitwijkprocedures beschikbaar zijn.
- De derde partij beschrijft de procedure voor systeemwijzigingen die impact (kunnen) hebben op de klant.

Welke maatregelen zijn er m.b.t. de omgang met verwijderbare media?

- Er dienen procedures te worden vastgesteld voor het beheer van verwijderbare media.
- Er dienen procedures te worden vastgesteld voor het op een veilige manier verwijderen van media als ze niet langer nodig zijn.
- Systeemdocumentatie dient te worden beschermd tegen onbevoegde toegang.
- Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik. In ieder geval indien er vertrouwelijke informatie is opgeslagen en/of licentieplichtige programmatuur op is geïnstalleerd.
- Er zijn richtlijnen voor het opbergen van papieren en computermedia. In ieder geval voor gevoelige of kritieke bedrijfsinformatie.
- Innamebeleid voor mobiele apparatuur, zoals laptops, pda’s, tablets en smartphones voor wanneer deze niet meer worden gebruikt.
- Encryptie op gegevens met het classificatielabel vertrouwelijk en zeer geheim.

Welke maatregelen zijn van toepassing op de uitwisseling van informatie?

- Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Vaststellen overeenkomsten voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- Beschermingsmaatregelen voor media die informatie bevatten tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
- Bescherming van informatie, die een rol speelt bij elektronische berichtuitwisseling.
- Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Een basisraamwerk met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
- Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.
- Omgang met sociale media beschrijven, met speciale aandacht voor het gebruik van Whatsapp extern en Signal intern. Zie hier voor het document Keuze en Gebruik Dienstverleningskanalen

11. Logische toegangsbeveiliging – maatregelen m.b.t. toegang tot IT omgevingen

Welke maatregelen zijn er m.b.t. identificatie, authenticatie en autorisatie?

- De eigenaar van de data is bevoegd toegang te verlenen.

- Er worden in de regel geen ‘algemene’ identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts.
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke en Europese) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD, IRMA, eHerkenning en eIDAS).
- Wachtwoorden worden voor een beperkte periode toegekend (90 dagen). Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.[16]
- Eisen aan wachtwoorden zijn:
    - Accountlock-out
    - aantal minuten 30
    - aantal pogingen 3
    - reset van de lock-out pogingen 1440 minuten
    - Minimum wachtwoordlengte: 8-14 karakters (afhankelijk van normale eindgebruiker of beheeraccount);
    - Wachtwoordhistorie: 14-24 of meer wachtwoorden (afhankelijk van normale eindgebruiker of beheeraccount);
- MFA (multi factor authentication) is van toepassing op alle applicaties die via internet toegankelijk zijn voor medewerkers en waarin persoons- gegevens of bedrijfsgevoelige informatie verwerkt wordt. Dit zijn de classificaties ‘midden’ of ‘hoog’.
- De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
- Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).
- Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.
- Diverse leveranciers hebben afwijkende oplossingen voor MFA met als gevolg dat medewerkers met verschillende apps te maken krijgen, en waarbij herstellen van toegang bij verlies van het devices per applicatie verschilt. Om de risico`s die dit met zich meebrengt te beperken hebben wij de volgende uitgangspunten:
    - Tenzij een leverancier geen andere keus heeft (een vorm van MFA is beter dan geen MFA) staan we geen SMS meer toe als 2e factor. SMS is geen veilig kanaal voor het uitwisselen van gegevens, het kan te makkelijk gespoofed worden[17].
    - Een leverancier implementeert de TOTP[18] standaard voor MFA.
    - Als alternatief voor een MFA oplossing kan in sommige gevallen ook gekozen worden voor gefedereerd inloggen via de ADFS voorziening van de IRvN. Daar wordt MFA al afgedwongen. Een medewerker krijgt dan geen nieuwe credentials. Het nadeel is dat als de credentials van een medewerker uitlekken, of bij een gerichte aanval, er toegang verkregen kan worden tot een grote hoeveelheid aan applicaties.
    - Als standaard app voor medewerkers voor het opslaan van de geheime sleutel gebruiken we de Microsoft Authenticator app[19]. Deze app is al in gebruik voor authenticatie met MFA op het domein van de IRvN en werkt ook goed met de TOTP standaard.
    - We dwingen af (via Intune) of communiceren naar gebruikers hoe ze de app kunnen backuppen naar hun iCloud account[20]. Dit zorgt ervoor dat bij verlies van het toestel een gebruiker makkelijk de diversie geheime sleutels weer kan restoren.

Voor ‘high profile targets’ zoals de gemeentesecretaris, concernmanagers of medewerkers met toegang tot financiële systemen willen wij een pilot starten met FIDO2/WebAUthn om te zien of het in de praktijk bruikbaar is. De FIDO2

[16] Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleids document van de gemeente.
[17] https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/
[18] https://www.forumstandaardisatie.nl/open-standaarden/totp
[19] https://www.microsoft.com/en-us/account/authenticator
[20] https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-backup-recovery

standaard[21], in combinatie met WebAuthn[22] is ook een MFA oplossing, maar in dit geval wordt er wel een cryptografische koppeling gemaakt tussen de applicatie en het MFA token.

Het MFA token wordt niet meer opgeslagen in een applicatie, maar in een hardware oplossing (een FIDO2 key).
Bij het vrijgeven van een MFA token valideert de FIDO2 key of de vragende applicatie inderdaad de applicatie is die het token heeft uitgegeven.
Deze constructie helpt tegen aanvallen waarbij een gebruiker verleid wordt authenticatie gegevens in te vullen op een nagemaakt website.

Welke maatregelen nemen wij bij het verlenen van toegang aan derden?

- De gemeente kan een externe partij toegang verlenen tot het netwerk. Zie voor de werkwijze de Procedure Netwerktoegang voor Externen van de iRvN. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij uitdrukkelijk overeengekomen.
- De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.
- Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken. Het uniek identificeren van elke gebruiker tot één persoon;
- Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde; Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek;
- De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats. Dit is een terugkererende taak van de kwaliteitsmedewerker. Stadscontrol toetst hier op.

Welke maatregelen kennen wij m.b.t. mobiel en thuiswerken?

- Voor mobiel werken en thuiswerken gelden dezelfde informatiebeveiligingseisen als voor andere manieren van werken. Medewerkers dragen er met name zorg voor dat de vertrouwelijkheid van informatie bij mobiel en thuiswerken niet in het geding komt. Meer informatie hier over is te vinden in het Thuiswerkbeleid.
- Voor de beveiliging van mobiele devices gelden specifieke eisen. Deze zijn opgenomen in het mobiele devices-beleid.

Welke maatregelen nemen we nog meer op het organisatorische vlak?

- Toetsing op het informatiebeveiligingsbeleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start en eind architectuur (PSA en PEA[23]).
- Projecten met een hoog risicoprofiel vallen onder toezicht van de afdeling Personeel Informatie en Facilitair. Toetsing op architectuur en informatiebeveiliging is hier onderdeel van.
- Projectmandaten worden ten behoeve van behandeling in overleg (onder meer) voorzien van een advies op informatiebeveiliging.
- In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

Welke specifieke beheersmaatregelen zijn er voor Suwinet?

Zie Hoofdstuk 16 Beveiligingsbeleid gebruik Suwinet

[21] https://fidoalliance.org/fido2/
[22] https://en.wikipedia.org/wiki/WebAuthn
[23] Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince2

12. Verwerving, ontwikkeling en onderhoud van informatiesystemen – maatregelen op het vlak van inkoop van IT

Welke maatregelen zijn er t.b.v. de specificatie van beveiligingseisen in een traject?

- In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen;
- In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten. Waar mogelijk wordt gebruikt gemaakt van bestaande richtlijnen (bijv. secure codingguidelines[24])
- Bij aanschaf van producten wordt een proces gevolgd waarbij een risico analyse en daaruit volgende beveiligingseisen een onderdeel zijn van de specificatie.
- Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[25] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria).
- Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke 'achterdeurtjes'.

Welke maatregelen zijn er m.b.t. de juiste verwerking in applicaties (vanaf integriteits niveau "beschermd")?

- Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-injection) en inconsistentie van gegevens.
- Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
- Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.
- Stapelen van fouten wordt voorkomen door toepassing van 'noodstop' mechanismen.
- Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid (vanaf vertrouwelijkheidsniveau "bedrijfsvertrouwelijk")beschikbaar gesteld worden (bijv. beveiligd printen).
- Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need-to-know).

Welke maatregelen nemen wij m.b.t. cryptografie in een traject (vertrouwelijke gegevens)?

- De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
- Bij de inzet van cryptografische producten volgt naast een afweging van de waarde van de informatie ook een analyse van de risico's aangaande locaties, processen en behandelende partijen.
- De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
- In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
- De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.

[24] Voor voorbeelden van secure coding guidelines, zie http://www.cert.org/secure-coding/ of bijvoorbeeld ook OWASP
[25] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

- De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
- Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
- Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid.

Welke maatregelen nemen wij ter bescherming van systeembestanden?

- Alleen geautoriseerd personeel kan functies en software installeren of activeren.
- Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
- Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
- Er worden alleen door de leverancier[26] onderhouden (versies van) software gebruikt.
- Van updates wordt een log bijgehouden.
- Er is een rollbackstrategie.

Welke maatregelen nemen wij ter bescherming van testdata?

- Het gebruik van kopieën van operationele databases voor testgegevens wordt vermeden. Indien toch noodzakelijk, worden de gegevens zoveel mogelijk geanonimiseerd en na de test zorgvuldig verwijderd.

Welke maatregelen nemen wij bij het doorvoeren van wijzigingen?

- Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL[27] en, voor applicaties ASL.
- Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen (test en acceptatie).
- Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

Welke maatregelen zijn er om uitlekken van informatie te voorkomen?

- Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats.[28]
- Er dient een proces te zijn om te melden dat (persoons) informatie is uitgelekt.

Welke maatregelen bestrijden technische kwetsbaarheden?

- Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten aan de Informatiebeveiligingsdienst, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
- Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
- Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.
- Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst (IBD) of een andere CERT zoals bijvoorbeeld het NCSC. Gemeente Nijmegen is aangesloten bij de IBD.

[26] Dit kan ook een interne leverancier zijn.

[27] Information Technology Infrastructure Library, zie http://www.itil-officialsite.com

[28] Het gaat hier dan om informatie die zich daar voor leent. Encrypted informatie is niet zondermeer te scannen.

13. Beveiligingsincidenten – registreren en leren van incidenten

Welke maatregelen zijn er om melding en registratie van incidenten te bevorderen?

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de informatiebeveiligingsfunctionarisen van de gemeente. Dit gaat via een melding bij de ICT Servicedesk.
- Beveiligingsincidenten die worden gemeld bij de service desk, worden als zodanig geregistreerd en voorgelegd aan de (plaatsvervangend) CISO dan wel FG. Voor de afhandeling wordt de reguliere rapportage en escalatielijn gevolgd.
- Afhankelijk van de ernst van een incident is er een meldplicht bij het Autoriteit Persoonsgegevens vanaf 1 januari 2016.
- Afhankelijk van de ernst van een incident wordt het crisisteam bij elkaar geroepen.
- Incidenten worden jaarlijks gerapporteerd door de CISO in de Rapportage Informatiebeveiliging.
- De taken van de CISO (en de FG) bij Informatiebeveiligingsincidenten staan beschreven in de pre-grip takenkaart.
- Bij grootschalige incidenten wordt indien nodig de CISO/FG gewaarschuwd conform de GRIP structuur.

Welke maatregelen zorgen voor alarmering?

- Bij grootschalige incidenten wordt gehandeld en opgeschaald volgens de GRIP structuur. Er is een takenkaart CISO/FG voor GRIP omstandigheden. De CISO/FG wordt opgeroepen ter advisering van het Hoofd Informatie (CIO).

Alarm fase	Kenmerk	Impact	Opschaling	Bijzonderheden
1	Lokaal incident bij één afdeling.	Oplosbaar probleem: bronbestrijding.	In beginsel niet. Probleem wordt opgelost door de afdeling Personeel Informatie en Facilitair.	Melding aan de CISO
2	Incident bij meer dan één organisatie onderdeel	Nog steeds een geïsoleerd probleem: bron - + effectbestrijding.	In beginsel niet. Probleem wordt opgelost door de afdeling Personeel Informatie en Facilitair.	Melding aan de CISO. Melding bij IBD indien nodig. Interne communicatie is optioneel.
3	Concernbreed incident (en mogelijk andere organisaties)	Impact op dienstverlening wordt echt ervaren.	Kernteam komt bij elkaar. Afhankelijk van het incident (impact) wordt geëscaleerd. Bestuur, CIO en management worden geïnformeerd.	Melding aan de CISO. Melding bij IBD (indien nodig) afdeling Interne (en externe) communicatie is vereist.
4	Incident is concern overstijgend (landelijk)	Impact op dienstverlening is manifest.	Mogelijk treedt de GRIP structuur in werking (GRIP Rijk). Het kernteam is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein).	Er is sprake van landelijke opschaling via de technische lijn (IBD → NCSC) of via de maatschappelijke lijn (Nationaal Crisis Centrum).

Welke maatregelen gelden bij de opschaling conform de GRIP-structuur

Opschaling is cruciaal bij een ramp of crisis. De zogeheten GRIP-structuur speelt daarbij een belangrijke rol. Opschaling vindt plaats op basis van de ernst en omvang van de gebeurtenis. Bij opschaling kunnen de verantwoordelijkheden en bevoegdheden wijzigen. Feitelijk richt de procedure zich op het zoeken naar het meest geschikte afstemmingsniveau. GRIP incidenten zijn meestal geen informatiebeveiligingsincidenten maar veiligheidsincidenten.

GRIP-1

Bij dagelijkse incidenten handelen de diensten zelf de zaken af. In sommige gevallen vinden één of meer partijen het handig en verstandig ter plaatse afstemming te organiseren en te formaliseren. Dat noemen we GRIP-1: een situatie waarvoor een Commando Plaats Incident (CoPI) wordt ingericht.

GRIP-2

Als de situatie wat omvangrijker is en er buiten de plaats van het incident ook maatregelen nodig zijn (bijvoorbeeld ten aanzien van de afvoer van gewonden of een dreigende rookwolk), kan worden opgeschaald naar GRIP-2. Naast het CoPI

wordt dan een operationeel team gevormd; meestal op regionaal niveau onder de noemer ROT (Regionaal Operationeel Team). Dit team biedt ondersteuning aan het CoPI.

GRIP-3

Situaties waarbij er sprake is van (dreigende) maatschappelijke onrust, komen in aanmerking voor GRIP-3. In deze situaties komt de burgemeester in beeld. Hij of zij laat zich ondersteunen door een gemeentelijk beleidsteam (GBT) met vertegenwoordigers van de belangrijkste betrokken organisaties.

GRIP-4

Omdat niet elke ramp of crisis zich aan de gemeentegrenzen houdt, is er ook nog een GRIP-4. Dan gaat het om situaties waarin de ramp of crisis de grenzen van een gemeente overstijgt (of als de betreffende gemeente de situatie niet alleen aankan). In zo'n situatie, zo is in de wet bepaald, krijgt de voorzitter van de veiligheidsregio de leiding en wordt er een regionaal beleidsteam (RBT) gevormd.

GRIP-5

Wanneer bij een incident of de vrees daarvoor meerdere veiligheidsregio's betrokken zijn, kunnen de voorzitters van deze veiligheidsregio's in gezamenlijkheid opschalen naar GRIP 5. De bronregio neemt in principe de coördinerende rol op zich. De voorzitter van de bronregio neemt niet de bevoegdheden van de overige betrokken voorzitters veiligheidsregio over.

GRIP-Rijk

Wanneer de nationale veiligheid in het geding is en er behoefte is aan sturing door het Rijk kan de Ministeriële Commissie Crisisbeheersing (MCCb) GRIP Rijk afkondigen. GRIP Rijk kan van kracht zijn in combinatie met GRIP 1 t/m 5 of zonder dat er sprake is van opschaling in de veiligheidsregio.

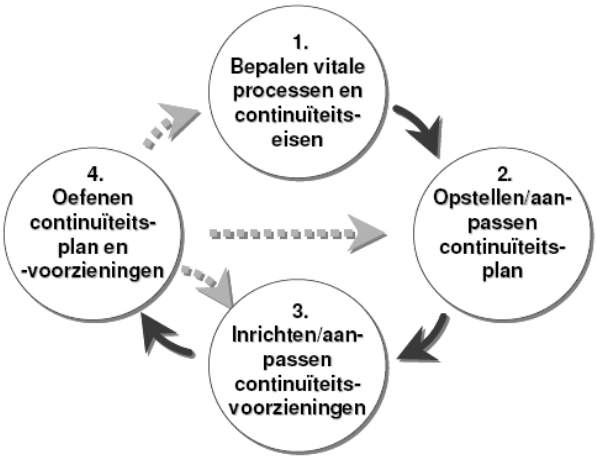
14. Bedrijfscontinuïteit – maatregelen die snel herstel van de bedrijfsvoering bevorderen

Welke maatregelen ondersteunen het herstel?

- De organisatie voert een business impactanalyse uit. Afhankelijk van de bevindingen worden vervolgacties gepland. De gemeente heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In de continuïteitsplannen wordt minimaal aandacht besteed aan:
    - risico's;
    - identificatie van essentiële procedures voor bedrijfscontinuïteit;
    - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
    - veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
    - prioriteiten en volgorde van herstel en reconstructie;
    - documentatie van systemen en processen;
    - kennis en kundigheid van personeel om de processen weer op te starten.
- Er worden minimaal jaarlijks oefeningen of testen gehouden om het plan te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten wordt het plan bijgesteld en wordt de organisatie bijgeschoold.

Welke voorwaarden veronderstellen we hierbij?

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.
Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.



Figuur 2:● BCM Cyclus

15. Naleving – maatregelen om verantwoording te ondersteunen

Welke maatregelen zijn er als het gaat om het verbeteren van processen?

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.
- Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402 Type 1 of Type 2 verklaring).
- Periodiek wordt de kwaliteit van informatieveiligheid onderzocht door auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Dit kan in opdracht van de CIO (Chief Information Officer, Hoofd Informatievoorziening) plaatsvinden, maar ook in opdracht van andere stakeholders zoals bijvoorbeeld de Raad. Jaarlijks worden diverse audits, assessments en zelfevaluaties gepland. De bevindingen worden door de CISO gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt door de CISO gerapporteerd over informatieveiligheid aan de hand van de Verklaring Van Toepasselijkheid (= VVT).
- Er wordt een beveiligingsdocumentatiedossier door de CISO aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan voor de diverse audits, assessments en zelfevaluaties.

Welke maatregelen zijn er op het wettelijke vlak?

- Een overzicht van relevante wet en regelgeving is te vinden bij 15.1.1 Identificatie van toepasselijke wetgeving en contractuele verplichtingen. Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens.
- Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.
- Bij het (laten) vervaardigen en installeren van programmatuur, wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar mogelijk op rusten, niet worden geschonden.

16. Takenoverzicht privacy- en informatiebeveiligingsrollen (profielen)

In aanvulling op Hoofdstuk 6 gelden de volgende profielen voor de daar genoemde privacy- en informatiebeveiligingsrollen:

Concernmanager – eigenaar

- Stelt gezamenlijk met het GMT het informatiebeleid, het informatiebeveiligings- en privacybeleid vast.
- Vertaalt het informatiebeleid, het informatiebeveiligings- en privacybeleid naar doelstellingen voor de afdeling en het domein (bedrijfsfunctie) van de eigen afdeling.
- Is verantwoordelijk voor de informatievoorziening en/of de informatiesystemen die binnen het domein (bedrijfsfunctie) van de eigen afdeling vallen.
- Is (mede-)verantwoordelijk voor de integrale informatiebeveiliging van en privacybescherming binnen zijn of haar organisatieonderdeel.
- Bepaalt de waarde van de informatievoorziening en/of de informatiesystemen voor de bedrijfscontinuïteit en de dienstverlening (classificatie op beschikbaarheid, integriteit en vertrouwelijkheid).
- Stelt voldoende middelen beschikbaar voor het beheren van informatie en het uitvoeren van informatiebeheers-, informatiebeveiligings- en privacybeschermingsmaatregelen, afhankelijk van risicoacceptatie.
- Neemt besluiten over informatiebeheer-, informatiebeveiligings- en privacybeschermingsmaatregelen (afhankelijk van kosten en risicoacceptatie) en ziet er op toe dat deze worden uitgevoerd (bijv. dat een wachtwoordmanager gebruikt wordt).
- Stuurt op informatiebewustzijn en naleving van regels en richtlijnen en laat hier in voorbeeld gedrag zien.
- Zorgt dat medewerkers opgeleid zijn in het gebruik van informatiesystemen en andere informatiebronnen en weten wat van hen verwacht wordt in het kader van informatiebeheer, informatiebeveiliging en privacybescherming.
- Heeft bij extern beheerde informatievoorziening en informatiesystemen de rol van opdrachtgever.
- Wijst gepaste verantwoordelijkheden, bevoegdheden en autorisaties toe zodat de informatievoorziening en/of de informatiesystemen voldoen aan de gestelde eisen.
- Delegeert verantwoordelijkheid voor specifieke beheersmaatregelen aan beheerders en andere medewerkers in de vorm van een rol of taak (met de benodigde autorisaties).
- Mandateert vanuit het GMT verantwoordelijkheid voor besluiten over nieuwe ICT-voorzieningen, wijzigingen in en uitfasering van ICT-voorzieningen met beperkte impact op financiën en dienstverlening aan de CIO.

CIO – Chief Information Officer

- Is op hoofdlijnen op de hoogte van nieuwe ontwikkelingen op ICT-gebied voor de gemeente.
- Ontwikkelt een strategische visie op informatievoorziening (DIB) en legt deze voor aan het GMT.
- Toetst nieuwe ICT-voorzieningen en wijzigingen in ICT-voorzieningen (in ITIL termen: wijzigingsbeheer) op basis van beleid.
- Besluit gemandateerd over nieuwe ICT-voorzieningen, wijzigingen in en uitfasering van ICT-voorzieningen met beperkte impact op financiën en dienstverlening.
- Adviseert naar afdelingshoofden bij besluitvorming rond nieuwe ICT-voorzieningen en wijzigingen in ICT-voorzieningen met grote impact op financiën en dienstverlening.
- Adviseert afdelingshoofd PIF als eigenaar (conform definitie ISMS) van ICT gerelateerde bedrijfsfuncties gegevensbeheer, archief- en informatiebeheer, automatiseringsmanagement en informatiseringsmanagement
- Is opdrachtgever van de IRvN.
- Voert regie over (ISMS) bedrijfsmiddelen die beheerd worden door de IRvN (IaaS, PaaS, Netwerk)
- Toetst in de context van regievoering het classificatieniveau van ICT-bedrijfsmiddelen en laat de registratie van ICT-bedrijfsmiddelen aanpassen waar nodig.
- Is betrokken bij het definiëren van toegangsbeperkingen voor bedrijfsmiddelen.
- Is eerste aanspreekpunt van de IRvN in een cybercrisis (in samenwerking met de CISO, situatieafhankelijk).
- Is deelnemer gemeentelijk crisisteam.

CISO – Chief Information Security Officer

- Is op hoofdlijnen op de hoogte van dreigingen en de risico`s voor de gemeente.

- Ontwikkelt een strategische visie op informatiebeveiliging (informatiebeveiligingsbeleid) en legt deze voor aan het GMT (rol concernmanager – eigenaar).
- Beoordeelt op hoofdlijnen het informatiebeveiligingsbeleid van ketenpartners en leveranciers.
- Adviseert afdelingshoofden en medewerkers over informatiebeveiliging, met name bij gegevensverwerkingen op afdelingsoverstijgend strategisch niveau.
- Adviseert bij het op- en vaststellen van richtlijnen, procedures en audit criteria en zorgt voor vaststelling door het GMT.
- Stelt een controleplan IT op.
- Controleert en accepteert het ISMS (als eindverantwoordelijke).
- Bewaakt uitvoering van risico, oorzaak en gevolg analyses, dreigingen assessments en baselines en de maatregelen en taken die hier uit volgen, regulier, voortvloeiend uit (verwerkers-)overeenkomsten of naar aanleiding van datalekken en incidenten.
- Plant en ondersteunt periodieke assessments en reguliere audits (accountant, DigiD).
- Rapporteert aan college en Raad over informatiebeveiliging.
- Coördineert een leerprogramma ten behoeve van security awareness.
- Is deelnemer aan gemeentelijk crisisteam.

SO – Security Officer

- Is op de hoogte van nieuwe dreigingen en de risico`s voor de gemeente op tactisch niveau. Operationeel ondersteund door de IRvN. Beheert het register aan risico's en dreigingen en vult deze aan.
- Stelt op basis van het informatiebeveiligingsbeleid specifieke richtlijnen, procedures en audit criteria op en zorgt voor de invoering daarvan.
- Ondersteunt bij het behalen van informatiebeveiligingsdoelstellingen, bijvoorbeeld met het ontwikkelen van praktische instrumenten.
- Voert risico, oorzaak en gevolg analyses (bijvoorbeeld tijdens intake proces of als zelfstandige Business Impact Assessments) uit met afdelingshoofden (eigenaren) en andere stakeholders.
- Ondersteunt een leerprogramma voor security awareness.
- Adviseert medewerkers over (de technologie van) informatiebeveiliging op casusniveau bijvoorbeeld op het vlak van verwerkersovereenkomsten. Stimuleert Privacy by Design en by Default.
- Analyseert de afhandeling van datalek meldingen en incidenten en stelt op basis hiervan verbetervoorstellen op.
- Is hoofdgebruiker en applicatiebeheerder van het ISMS.
- Zorgt voor periodieke rapportages uit het ISMS.
- Ondersteunt de ISMS gebruikers.
- Zorgt voor verbinding met de gemeentelijke en IRvN-beheerders.

FG – Functionaris Gegevensbescherming

- Is op hoofdlijnen op de hoogte van dreigingen en de risico`s voor de gemeente op het gebied van privacy.
- Ontwikkelt een strategische visie op privacybescherming (privacybeleid) en legt deze voor aan het GMT.
- Adviseert afdelingshoofden en medewerkers over privacybescherming, met name bij gegevensverwerkingen op overstijgend strategisch niveau.
- Adviseert bij het aan de hand van de doelstellingen formuleren van onderdelen van het privacybeleid met audit criteria.
- Bewaakt het opstellen van verwerkersovereenkomsten.
- Toetst de gemeente en partners/verwerkers in het kader van het voldoen aan wet- en regelgeving en de uitvoering van afspraken uit verwerkersovereenkomsten.
- Controleert de actuele compliance status en stelt daarvoor een controleplan gegevensverwerkingen op.
- Adviseert bij controleplan IT.
- Controleert en accepteert het PIMS (als eindverantwoordelijke).
- Stelt onderzoek in n.a.v. privacy klachten/signalen.
- Bewaakt uitvoering van risico, oorzaak en gevolg analyses op gebied van privacy (m.n. Data Protection Impact Assessments) en de maatregelen en taken die hier uit volgen.

- Controleert de afhandeling van privacy en datalek meldingen en incidenten en monitort de opvolging van de gemaakte afspraken.
- Coördineert een leerprogramma ten behoeve van privacy awareness.
- Contactpersoon en spreekbuis van de Autoriteit Persoonsgegevens.
- Rapporteert aan College en Raad over privacybescherming.

PO – Privacy Officer

- Is op de hoogte van (de actualiteiten van) het privacy recht en de verplichtingen die hieruit voortvloeien voor de organisatie.
- Stelt op basis van het privacybeleid specifieke richtlijnen, procedures en audit criteria op en zorgt voor de invoering daarvan.
- Adviseert medewerkers op het gebied van privacy bescherming op casusniveau. Stimuleert Privacy by Design en by Default.
- Adviseert bij het uitvoeren van Data Protection Impact Assessments.
- Adviseert bij het opstellen van verwerkersovereenkomsten.
- Ondersteunt een leerprogramma voor privacy awareness.
- Handelt verzoeken in het kader van rechten van betrokkenen af.
- Onderzoekt privacy klachten/signalen.
- Houdt het register van verwerkingen bij, inventariseert gegevensverwerkingen.
- Voert het controleplan gegevensverwerkingen uit.
- Is hoofdgebruiker en beheerder van het PIMS.
- Ondersteunt de PIMS gebruikers.
- Analyseert de afhandeling van privacy en datalek meldingen en stelt op basis hiervan verbetervoorstellen op.
- Zorgt voor verbinding met en ondersteuning van de Privacy Ambassadeurs.

Archiefinspecteur

- Ziet toe op en adviseert over wettelijke regelingen en voorzieningen op grond van de Archiefwet.
- Ziet toe op en adviseert over de juiste toewijzing van verantwoordelijkheden en mandaten in het kader van de Archiefwet.
- Toetst de informatievoorziening en (nieuwe) informatiesystemen en fysieke ruimtes waarbinnen deze functioneren op risico's voor de archieffunctie.
- Ziet toe op en adviseert over de juiste maatregelen n.a.v. gebeurtenissen welke impact kunnen hebben op gegevensverwerkingen en informatiebeheer, met name op het gebied van archiefwaardige informatie.
- Ziet toe op en adviseert over een juiste uitvoering van het beleid op gebied van bewaren en vernietigen van informatie, zoals vastgelegd in selectielijsten en het register van verwerkingen.
- Ziet toe op en adviseert over de preventie en repressie van calamiteiten waarbij schade aan archiefwaardige informatie kan of is ontstaan.
- Ziet toe op en adviseert over openbaarheidsbeperkingen van over te brengen en overgebrachte archieven, alsmede ontheffingen daarop.
- Rapporteert op gebied van informatiebewustzijn aan het college en Raad.
- Houdt actualiteiten bij op het gebied van archiefrecht, selectie en waardering en mogelijke archiveringsverplichtingen voor de organisatie.
- Stimuleert Archiving by Design en by Default.
- Draagt bij aan het bijhouden van het register van verwerkingen.
- Ziet mede toe op voorlichting en training op gebied van informatiebewustzijn en privacy.

Beheerder (Informatie-, data-, functioneel ICT-, technisch)

- Heeft een uitstekende kennis van de informatievoorziening, informatiesystemen en evt. de ruimtes waarbinnen deze functioneren.
- Draagt binnen het gemeentelijk beleid zorg voor de inrichting van informatie, data en/of informatiesystemen en evt. de ruimtes waarbinnen deze functioneren en voert de regie op het kwalitatief beheer hiervan.

- Adviseert vanuit beheers-, uitvoerings- en gebruikersperspectief bij de ontwikkeling van nieuw beleid en nieuwe producten op het beheersgebied en ondersteunt bij de implementatie daarvan.
- Ondersteunt de eigenaar bij het bepalen van de waarde van de informatievoorziening en/of het informatiesysteem.
- Draagt zorg voor het optimaliseren van werkwijzen, procedures en instrumenten op het gebied van informatievoorziening, informatiesystemen en evt. de ruimtes waarbinnen deze functioneren; ontwikkelt in dat kader de regels en instructies t.b.v. de uitvoeringspraktijk.
- Verzorgt coaching, (groeps-)instructies en ondersteuning op het gebied van informatievoorziening en informatiesystemen en verzorgt het gebruikersbeheer van informatiesystemen.
- Beheert de registratie en documentatie van de informatievoorziening en/of het informatiesysteem en zorgt dat de registratie overeenkomt met de actuele situatie.
- Ondersteunt bij de uitvoering van informatiebeveiligings-, archief- en privacybeschermingsmaatregelen of voert deze zelf uit (bijv. beheer toegangsrechten en autorisaties).
- Definieert toegangsbeperkingen op basis van vastgestelde rollen en verantwoordelijkheden en koppelt deze aan medewerkers die het informatiesysteem gebruiken.
- Beoordeelt kwetsbaarheden in informatiesystemenen en evt. de ruimtes waarbinnen deze functioneren en rapporteert hierover.
- Behandelt (mogelijke) gebeurtenissen en incidenten op gebied van privacy en informatiebeveiliging en zorgt dat deze behandeld kunnen worden en ondersteunt bij de afhandeling van verzoeken in het kader van rechten van betrokkenen.
- Ondersteunt bij de uitvoering van informatiebeveiligings-, archief- en privacyassessments en audits.
- Coördineert het veilig uitfaseren, verplaatsen, verwijderen en/of vernietigen van informatie en informatiesystemen of voert deze handelingen zelf uit.
- Legt verantwoording af aan het College over het beheer van informatie en/of informatiesystemen, evt. de ruimtes waarbinnen deze functioneren en de omgang met het uitgeoefende toezicht hierover.

17. Beveiligingsbeleid gebruik Suwinet

Suwinet Inkijk is een middel voor overheidsorganisaties om persoonsgegevens die bij verschillende overheidsinstanties zijn opgeslagen en daar worden beheerd, te delen en te raadplegen. In Suwinet zijn geen gegevens opgeslagen: het biedt vooral veilige toegang tot inkijken en tot delen. De informatie is echter alleen aanwezig bij de betreffende overheidsinstanties. Ook bij het raadplegen en delen van de informatie is het van belang de veiligheid van de informatie te waarborgen. De gegevens die je kunt inzien zijn alleen die gegevens die nodig zijn voor je wettelijke taak. Niet meer, niet minder. Het veilige gebruik van Suwinet wordt geborgd door logs van alle raadplegingen. Daarnaast geldt ook voor Suwinet het informatiebeveiligingsbeleid.

Het beveiligingsbeleid voor Suwinet Inkijk geldt onverkort voor alle gemeentelijke gebruik van van Suwinet. Daarmee strekt het beveiligingsbeleid zich uit over de inkijk voor Pw en DKD-inlezen, voor RMC en geldt eveneens voor toepassing binnen het domein van schuldhulpverlening.

Achtergrond gebruik in het kader van Pw en IOAW of IOAZ
Een gemeente heeft gegevens nodig van andere partijen voor de uitvoering van de Participatiewet, IOAW of IOAZ. Daarmee ontstaat een wettelijke grondslag tot het raadplegen van gegevens (art. 64 P-wet, art. 45 IOAW/ IOAZ). Partijen wisselen deze gegevens met elkaar uit via Suwinet (art. 62 Wet SUWI).

Daarnaast zijn er in de Algemene Verordening Gegevensbescherming (AVG) algemene regels over de verwerking van persoonsgegevens. Een belangrijke regel is dat gebruik van persoonsgegevens beperkt moet blijven tot de relevante gegevens (art. 5 AVG).

Bij de beoordeling of Suwinet gebruikt mag worden staan 3 vragen centraal:
- Valt deze taak onder de uitvoering van de P-wet/IOAW/IOAZ?
- Zo ja, staat deze taak/beoordeling expliciet beschreven in P-wet/IOAW/IOAZ?
- Zo ja, zijn de gewenste gegevens noodzakelijk voor de uitvoering van de uit te voeren taak uit de P-wet/ IOAW/IOAZ?

Als het antwoord op alle vragen “ja”, is raadpleging van Suwinet toegestaan.

Uitvoering Suwinet Inkijk voor Pw en IOAW of IOAZ
Raadpleging van Suwinet Inkijk geldt in elk geval voor de volgende taken:
- Vaststellen van de rechtmatigheid van de uitkering (art.17 lid 1 PW en art.53a lid 1 en 6 PW,
- art.14 IOAW/ IOAZ)
- Vaststellen definitieve einddatum van de uitkering na opschorting (art.17 lid 1 PW en art.53a lid
- 1 en 6 PW, art.14 IOAW/IOAZ)
- Re-integratie werkzaamheden, ook voor ex-gedetineerden mits het de doelgroep van de P-wet
- betreft (art. 7 lid 1 PW)
- Bijzondere bijstand (art. 35, 36, 36b PW)
- Taken rondom Bbz, Besluit bijstandsverlening zelfstandigen (art. 78f, 78g PW)
- Terugvordering en Verhaal, bijv. het raadplegen van de ex-partner voor vaststelling
- onderhoudsplicht (art. 58- 62i P-wet, art. 25-33 IOAW/IOAZ)

Soms wordt er op basis van de derde vraag een beperking aangegeven. Voor het vaststellen van kostendeling (art. 22a P-wet, art. 5 IOAW/IOAZ)) mag van de medebewoners (niet zijnde de partner van de klant of inwonende kinderen onder 18 jaar) alleen de pagina kostendelerstoets worden geraadpleegd. Het is niet toegestaan om van de medebewoner andere gegevens te raadplegen zoals uitkerings- of inkomensgegevens. Voor de Wet Inburgering mag het Inburgeringsportaal

via Suwinet gebruikt worden. De overige pagina's van Suwinet mogen voor pure inburgeringstaken niet gebruikt worden tenzij het een duaal traject betreft (inburgeraar volgt tevens re-integratie).
Voor ESF-aanvragen mag vooralsnog Suwinet gebruikt worden. Dit heeft SZW ook aangegeven in het Gemeentenieuws van SZW. Het Inlichtingenbureau heeft van SZW de opdracht gekregen te zoeken naar een nieuwe/andere informatieoplossing. Als die tot stand komt zal dat ook via het Gemeentenieuws van SZW worden gecommuniceerd en zal Suwinet niet meer gebruikt mogen worden voor ESF-aanvragen.

Achtergrond gebruik Suwinet in het kader van DKD inlezen
Het Inlichtingenbureau biedt gemeenten de mogelijkheid om DKD-klantgegevens digitaal in te lezen in de eigen, gemeentelijke applicatie. Daarnaast is het mogelijk om elektronische aanvraagformulieren gedeeltelijk, automatisch in te laten vullen, bijvoorbeeld bij het aanvragen van een bijstandsuitkering. Hiermee maakt DKD-Inlezen eenmalige gegevensuitvragen en het hergebruik van gegevens mogelijk. De gegevens mogen alleen gebruikt worden voor de uitvoering van de participatiewet taken. Zowel de huidige keten SLA als de komende versie staan het gebruik van DKD-Inlezen uitsluitend toe op gevalsbasis, per individueel BSN. Het op reguliere basis bevragen van de complete populatie is enkel toegestaan na het maken van concrete afspraken met de bronleveranciers, BKWI en het Inlichtingenbureau. In een beperkt aantal gevallen vindt dit ook plaats binnen de Gemeente Nijmegen. Daarbij gaat het met name om (automatische) koppelingen met Decos.

Achtergrond gebruik in het kader van RMC
Jongeren die voortijdig het onderwijs verlaten, zonder een havo-, vwo- of mbo diploma niveau 2 of hoger, hebben minder kansen op de arbeidsmarkt en dus op een eigen plek in de samenleving. Het terugdringen van het aantal voortijdige schoolverlaters (VSV'ers) staat hoog op de agenda van het Rijk en bij gemeenten, zo ook binnen het Rijk van Nijmegen.

Bureau Leerplicht Nijmegen voert voor de zeven gemeenten in het Rijk van Nijmegen de RMC-taken uit; gericht op het terugdringen van verzuim en uitval van leerlingen. Als jongeren toch het onderwijs verlaten zonder een startkwalificatie wordt bekeken of ondersteuning nodig is. Met gegevens uit de werk- en inkomensketen boeken de consulenten meer succes.

De regio Nijmegen heeft eind 2019 een aanvraag ingediend om deze gegevens voor de uitvoering van de RMC-functie te kunnen raadplegen via Suwinet-Inkijk. In de WEB (Wet Educatie en Beroepsonderwijs), WVO (Wet op het voortgezet onderwijs) en WEC (Wet op de expertise centra) is geregeld wanneer sprake is van een voortijdig schoolverlater. Een gemeente moet voor de uitvoering van haar wettelijke taak (bestrijden VSV) weten of een jongere aan de definitie voldoet en niet in onderwijs zit en geen werk of arbeidsovereenkomst heeft. Hiervoor kan een gemeente gebruik maken van gegevens uit SUWI.

UWV is op grond van artikel 5.9, eerste lid, onderdeel f, bevoegd en verplicht gegevens aan gemeenten te verstrekken ten behoeve van de uitvoering van artikel 118h van de Wet op het voortgezet onderwijs, artikel 8.3.2 van de Wet educatie en beroepsonderwijs en artikel 162b van de Wet op de expertisecentra in verband met de doorverwijzing van voortijdige schoolverlaters naar onderwijs of arbeidsmarkt.

Uitvoering Suwinet voor RMC
De RMC-medewerker heeft een aparte VSV-pagina in Suwinet-Inkijk. Op deze pagina zijn gegevens over personen, inkomensverhoudingen, uitkeringsaanvragen, uitkeringsverhoudingen, bijzondere bijstand en re-integratie zichtbaar. Het raadplegen van gegevens voor de RMC-functie is regio gebonden. Dat betekent dat alleen gegevens van jongeren die woonachtig zijn in de regio Rijk van Nijmegen kunnen worden geraadpleegd via Suwinet-Inkijk.

Achtergrond gebruik in het kader van Wet Gemeentelijke Schuldhulpverlening
Per 1 januari 2021 is de wet Gemeentelijke Schuldhulpverlening (Wgs) gewijzigd. Naast gewijzigde wetgeving is er per 1 januari ook een 'besluit gemeentelijke schuldhulpverlening' van kracht. De wet en het besluit hebben onder andere tot

doel om de inwoner tijdens de opstartfase van het schuldhulpverleningstraject te ontzorgen. Deze vroegsignalering van problematische schulden is onderdeel van de brede schuldenaanpak van het kabinet.

In het algemeen moeten de wet en het besluit de lastendruk voor de inwoner gaan verminderen. De voormalige Wgs ging er namelijk van uit dat inwoners zelf informatie aanleverden, zodat de schuldhulpverlener hier vervolgens een plan van aanpak voor schuldhulpverlening mee kon maken. Deze inlichtingenplicht werkte echter vertragend, leidde tot langere wacht- en doorlooptijden en soms ook tot uitval. Schuldhulpverleners worden met de gewijzigde Wgs in staat gesteld om mensen met schulden tijdig in beeld te krijgen en zo schuldhulpverlening aan te bieden.

Zij mogen meer informatie over inkomsten, schulden en vermogen uitwisselen met diverse instanties zodat de inwoner zelf minder gegevens behoeft aan te leveren. Binnen de Keten voor schulden en derdenbeslag wordt door een groot aantal overheidspartijen zoals SVB, LBIO, CJIB, gemeenten en waterschappen gewerkt aan de implementatie van de Wet vereenvoudiging beslagvrije voet en het traject dat moet leiden tot een betere gegevensuitwisseling over schulden (de wet Stroomlijning Keten voor Derdenbeslag). Dit alles in het kader van een brede schuldenaanpak.

Met de brede schuldenaanpak neemt het kabinet maatregelen om het aantal mensen met problematische schulden terug te dringen en mensen met schulden beter te helpen. Deze brede schuldenaanpak kent drie actielijnen: het voorkomen van problematische schulden, het ontzorgen en ondersteunen (snel en goed helpen) van burgers met schulden en een zorgvuldige en maatschappelijk verantwoorde incasso.

Uitvoering Suwinet inkijk voor de Wet gemeentelijke schuldhulpverlening
In de gewijzigde Wgs heeft de wetgever gemeenten de grondslag gegeven om inkomens en vermogensgegevens te raadplegen in het kader van het plan van aanpak schuldhulpverlening. Daarbij heeft de wetgever aangegeven dat het voor de hand ligt om hiervoor in de eerste instantie Suwinet te gebruiken. Voor de uitvoering van Wet gemeentelijke schuldhulpverlening (Wgs) kunnen schuldhulpverleners daarom vanaf de zomer 2021 Suwinet-Inkijk raadplegen. Via Suwinet-Inkijk worden persoonsgegevens die bij verschillende organisaties of basisregistraties zijn opgeslagen, gedeeld met andere overheidsorganisaties. Door Suwinet te raadplegen kunnen inwoners sneller en beter ondersteund worden in het kader van het plan van aanpak schuldhulpverlening. Ook kunnen de gegevens gebruikt worden voor de periodieke hercontrole schuldhulpverlening.

Functiescheiding:
Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor Suwinet. Het gaat dan met name over functiescheiding. Zo zijn de functies gebruik van Suwinet, beheer van autorisaties Suwinet, controle op het gebruik van Suwinet en beslissen over wie welke functies krijgt in Suwinet gescheiden. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt. De diverse functies noodzakelijk voor Suwinet en de overweging voor het toebedelen van de taken, profielen en rollen zijn schriftelijk vastgelegd, Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken.

- Uitvoering van taken (raadpleegfunctie Suwinet) ligt bij de reguliere gebruikers zoals klantmanagers,
- inkomensconsulenten en medewerkers Handhaving;
- Beheer van autorisaties en toegang verlenen tot Suwinet ligt bij enkele medewerkers van de ICT-afdeling (IRvN);
- Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, namens de security officer Suwinet) ligt bij kwaliteitsbeheer Zorg en Inkomen;
- Management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet) ligt bij de Security Officer (namens gemeentesecretaris en College).

- Taken Security Officer Suwinet:
    - Adviseert en rapporteert periodiek richting Directeur op het gebied van gebruik- en informatiebeveiliging Suwinet ;
    - Controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd;
    - Rapporteert beveiligingsincidenten richting verantwoordelijk afdelingshoofd en ziet toe op passende vervolgactie;

- Voert periodieke controles uit op een rechtmatig gebruik van Suwinet-inkijk;
- Doet voorstellen tot implementatie of aanpassing van plannen en werkprocessen op het gebied van de beveiliging;
- Fungeert als centraal aanspreekpunt op het gebied van beveiliging Suwinet;
- Bepaalt welke autorisaties een medewerker toegekend krijgt voor het uitvoeren van zijn of haar taken

- Taken Gebruikersbeheerder:
  - Toewijzen autorisaties:
    Het gebruik van Suwinet-Inkijk is voorbehouden aan de medewerkers van de afdelingen Zorg en Inkomen, Financiën (medewerkers Incasso en Gemeentebelastingen), Economische Zaken (Bbz) en Juridische Zaken (medewerkers bezwaar en beroep) De autorisaties voor Suwinet-Inkijk worden in beginsel per functiegroep toegekend. De medewerkers die een autorisatie voor Suwinet-Inkijk aanvragen, doen dat middels een webformulier. Daarbij moet de medewerker tevens een zorgvuldigheidsverklaring ondertekenen.
    Dit geldt ook voor extern personeel. De wijze waarop de autorisaties worden toebedeeld, gewijzigd of ingetrokken is nader vastgelegd in de bijlage 'Procedure autorisaties 2019'.
  - Communicatie:
  - Het beveiligingsbeleid/plan wordt aantoonbaar centraal beschikbaar gesteld voor alle gebruikers op Insite, de interne internetpagina. Medewerkers worden via Insite middels het beschikbaar stellen van het Beveiligingsplan op de hoogte gebracht van het bestaan, de aard en het doel van de logging van Suwi-raadplegingen en dat oneigenlijk gebruik sancties tot gevolg heeft. Vormen van een redactieraad die meerdere malen per jaar communiceert naar medewerkers over belang veilig gebruik Suwinet en waar mogelijk aansluit op actualiteit.

Beheersmaatregelen m.b.t. Suwinet

- Organisaties en werkwijzen veranderen continu. Dit kan van invloed zijn op de wijze waarop Suwinet wordt gebruikt. Daarom is het van belang om minimaal 3-jaarlijks het algemene informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet te evalueren en na te gaan of deze nog steeds voldoen aan de beveiligingseisen en –randvoorwaarden. Indien noodzakelijk zal het plan tussentijds worden aangepast.

- 'Whitelist':
  De gemeente Nijmegen hanteert de 'Whitelist'. Dit filter regelt dat medewerkers in beginsel alleen gegevens op kunnen vragen van de burgers die tot het klantenbestand behoren. Moet men voor de werkzaamheden ook regelmatig gegevens inzien van personen waar op dat moment (nog) geen dienstverleningsrelatie mee bestaat, dan kan, indien deze aan de functiegroep is toebedeeld, de zgn. escape-functie worden gebruikt. De medewerkers zijn over het gebruik van de whitelist/escapefunctie geïnformeerd en geïnstrueerd. Aan welke profielen de escapefunctie is toebedeeld en waarom is vastgelegd in 'Procedure autorisaties 2019'. De steekproefcontroles kunnen hiermee vanaf nu beperkt worden tot de raadplegingen waarvoor de escapefunctie gebruikt is.

Definities samenstelling whitelist die wekelijks wordt geüpload:
- Alle cliënten en partners Pw-Ioaw-Ioaz met een actuele uitkering algemene bijstand, geldlening BZ of periodieke bijzondere bijstand;
- Alle personen waarbij een aanvraag Inkomensondersteuning staat geregistreerd (tot jaar na datum besluit);
- Onderhoudsplichtigen met een registratie in de debiteurengroepen (onderhoudsplicht/verhaal) met een actueel saldo en verplichtingen;
- Alle debiteuren zonder een actuele uitkering met openstaand saldo op een vordering;
- Alle personen met een openstaande aanvraag levensonderhoud.

- Onderzoeksaanpak - Werkzaamheden
  Alle raadplegingen in Suwinet worden gelogd (bsn - datum – tijdstip – pagina's). Dit ten behoeve van controles op correct gebruik. Oneigenlijk gebruik heeft sancties voor de betreffende medewerker tot gevolg.

  De gemeente voert periodiek de volgende controles uit:

- Per kwartaal worden generieke rapportages opgevraagd van de rollen GSD en GB (Gemeentebelastingen) alsook RMC en schuldhulpverlening
- Gericht onderzoek (minimaal 2 maal per jaar):
  Uit de periodieke Suwinet-rapportages een aantal specifieke onderdelen benoemen die opvallen qua bijvoorbeeld tijdstip van het gebruik of hoogte van aantallen;
  Van deze onderdelen specifieke rapporten bij BKWI opvragen;
  Deze specifieke rapporten analyseren;
  Afhankelijk van de uitkomsten van deze analyse nadere onderzoeken uitvoeren en/of andere risico-onderdelen uit de meest actuele rapportage benoemen en hiervan vervolgens specifieke rapportages opvragen
  Rapporteren: bevindingen – aanbevelingen/beheersmaatregelen
  Afhankelijk van resultaten eventueel aanpassingen verrichten (proces - autorisaties - werkafspraken)
  Eventueel herhalen stap 1 enzovoorts
- Steekproefcontroles (minimaal 2 maal per jaar)
  Van één maand worden alle raadplegingen opgevraagd. Hierop wordt een aselecte steekproef uitgevoerd.
  Rapporteren: bevindingen – aanbevelingen/beheersmaatregelen
  Afhankelijk van resultaten eventueel aanpassingen verrichten (proces - autorisaties - werkafspraken)
  Eventueel herhalen stap 1 enzovoorts
- Controle op verlopen accounts (wachtwoord verlopen of langer dan 2 maanden niet ingelogd) wordt per kwartaal uitgevoerd. Deze accounts worden ingetrokken. Voor medewerkers die uit dienst treden wordt een lijst van applicaties gehanteerd die beëindigd moeten worden. Suwinet is hier gemeentebreed in opgenomen.
- Controle op aansluiting uitgegeven Suwinet-profielen en medewerkerslijst P&O vindt halfjaarlijks plaats. Er dient aangetoond te worden dat de uitgegeven profielen van alle medewerkers overeenkomen met hun formele functie en bijbehorende werkzaamheden. Via de gebruikersbeheerder wordt lijstwerk ontvangen van alle medewerkers die Suwinet gebruiken met daarin hun profielen. De gegevens uit de lijsten worden vergeleken met de functies. Waar niet direct helder is of het profiel akkoord is voor de functie wordt nader onderzoek verricht.
  Rapporteren: bevindingen – aanbevelingen/beheersmaatregelen
  Afhankelijk van resultaten eventueel aanpassingen verrichten (proces - autorisaties - werkafspraken)
- Controle op aansluiting te raadplegen pagina's per profiel met autorisatiematrix.
  Autorisatiematrix geeft aan welke pagina's per profiel geraadpleegd mogen worden. Halfjaarlijks wordt per profel gecontroleerd of de te raadplegen pagina’s overeenkosmen met de matrix.
- Controle op veranderingen in de whitelist en het voldoen aan bovenstaande definitie.

De rapportages over de bevindingen worden door kwaliteitsbeheer Z&I doorgegeven aan de Security Officer en het afdelingshoofd Z&I. Waar nodig is dit onderwerp van gesprek tussen beide.

18. Verklarende begrippenlijst

Begrip	**Verklaring**
2FA	Twee factor authenticatie vereist twee manieren om je als gebruiker kenbaar te maken. Meestal gaat het om een wachtwoord (iets dat je weet) en een toegangscode (iets dat je hebt).
3 lines of defense	Een organisatie model waarbij bepaalde rollen en verantwoordelijkheiden zijn toegewezen aan lagen in de organisatie, met name op het vlak van eigenaarschap, ondersteuning en control.
ADFS	Active Directory Federation Services. Een Microsoft systeem waarmee gebruikers kunnen inloggen op systemen in de cloud terwijl ze gebruik maken van hun bestaande bedrijfsinloggegevens.
Audittrail	Stelt een onderneming of toezichthouder in staat om transacties administratief te volgen en te controleren. Een controlespoor kan vooraf gaan aan een financiële transactie, maar bijvoorbeeld ook aan het aangaan van een nieuwe klantrelatie. Vaak is een audit trail wettelijk verplicht.

AVG	Algemene verordening gegevensbescherming (Engels: General Data Protection Regulation (GDPR)) is de Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. De uitvoering van de verordening is bepaald door de Uitvoeringswet (UAVG).
BAG	Basisregistratie Adressen en Gebouwen. Onderdeel van geografische (GEO) informatie.
BBN	Basisbeveiligingsniveau. Classificatie niveaus behorend bij de BIO (zie verder op), toe te passen op gemeentelijke informatiesystemen.
BGT	Basisregistratie Grootschalige Topografie. Onderdeel van geografische (GEO) informatie. Digitale kaart van Nederland waarop gebouwen en terreinen eenduidig zijn vastgelegd.
BIG	Baseline Informatiebeveiliging voor Gemeenten (2013 – 2019). Van ISO 27001/2 afgeleid normenkader toegesneden op Nederlandse gemeenten.
BIO	De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Vervolg op de BIG om de samenwerking tussen overheidslagen in Nederland te verbeteren. Vanaf 2020
BKWI	Bureau Keteninformatiesering Werk en Inkomen. Onderdeel van UWV in opdracht van het Ministerie van Sociale Zaken. Bevorderen samenwerking tussen overheidsorganisaties.
BRO	Basisregistratie Ondergrond. Onderdeel van geografische (GEO) informatie. Centrale registratie van gegevens mbt de ondergrond zoals grondwater informatie.
BRP	Basisregistratie Personen.
CAR-UWO	Collectieve Arbeidsvoorwaarden Regeling – en Uitwerkingsovereenkomst. Arbeidsvoorwaarden voor gemeenten.
CERT	Computer emergency response team. Een gespecialiseerd team van ICT medewerkers dat handelt bij een incident met computers of netwerken om de schade te beperken en de dienstverlening snel te herstellen.
Checksum	Een controlegetal. Dergelijke getallen zijn bedoeld om een systematische redundantie te creëren in gegevens om het invoeren, lezen, schrijven en verzenden ervan te controleren, op een wijze die efficiënter is dan alles twee keer te doen. Bijvoorbeeld door voor en na de te controleren actie een resultaat te berekenen (compacter dan de gegevens zelf) en de twee resultaten te vergelijken.
CIO	Chief Information Officer gaat over de informatievoorziening van de organisatie
CISO	Chief Information Security Officer gaat over de informatie beveiliging in de organiatie
Cloud	Programmatuur die niet op het bedrijfsnetwerk beheerd wordt maar beschikbaar gesteld wordt bij een leverancier, via het internet, bevindt zich in de “cloud”.
CPU	Central processing unit. De processor (centrale verwerkingseenheid) in een computer
CSIRT	Cyber security incident response team. Team van gespecialiseerde ICT medewerkers die reageren op IT beveiligingsincidenten.
Datacenter	Een faciliteit waar ICT apparatuur onder gecontroleerde omstandigheden wordt beheerd.
Delegeren	Delegeren daarentegen betekent wel het overdragen van bevoegdheden, inclusief de verantwoordelijkheid.
DigiD	Syteem van de Nederlandse overheid waarmee de identiteit van een burger vastgesteld kan worden.
DKIM	DomainKeys Identified Mail (DKIM) is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden.
DMARC	DMARC maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein.
DNSSEC	DNSSEC staat voor Domain Name System Security Extensions, Het DNS protocol zorgt voor de vertaling van een domeinnaam naar een IP-adres. DNSSEC voorziet de DNS records van een digitale handtekening, zodat de aanvrager kan controleren of de informatie die terug komt, authentiek is.

DPIA	Data protection impact assessment. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.
eHerkenning	Een gestandaardiseerd inlogsysteem voor organisaties waarmee hun identiteit en bevoegdheid wordt vastgesteld. Soort DigiD voor bedrijven.
EIDAS	Electronic Identification Authentication and trust Services is een Europese verordening die een kader moet bieden voor veilige, betrouwbare en gebruiksvriendelijke electronische transacties binnen de EU.
FG	Functionaris Gegevensbescherming houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
FIDO2/WebAuthn	Fast Identity Online 2 is een standaard ontwikkeld door de FIDO alliantie die een veilige manier van inloggen moet bieden zonder het gebruik van wachtwoorden (en alle risico`s van dien). WebAuthn is de manier waarop webbrowsers deze standaard gebruiken.
GEMMA2	De tweede versie van de Gemeentelijke Model Architectuur. Hierein staat beschreven welke functies, koppelvlakken en standaarden gemeenten gebruiken.
GIBIT	Gemeentelijke Inkoopvoorwaarden bij IT. Deze uniforme inkoopvoorwaarden helpen gemeenten bij het professionaliseren van de inkoop van ICT-diensten en –producten.
GRIP (1-5)	Gecoordineerde Regionale Incidentbestrijdingsprocedure. Niveau 1 t/m 5, afhankelijk van de schaalgrootte en de benodigde middelen.
Hosting	Het huren van opslag, rekenkracht en geheugen van een server (computer) in een datacenter.
IBD	Informatiebeveiligingsdienst voor gemeenten. Onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De sectorale CERT/CSIRT voor alle Nederlandse gemeenten.
Interceptie	Onderscheppen van communicatie uit het netwerk.
IRMA	I Reveal My Attributes. Een platform ontwikkeld door de stichting Privacy by Design om de benodigde attributen aan te kunnen tonen voor het doen van transacties (en andere niet). Ook gebruikt IRMA geen tussenpersonen waardoor alleen de betrokkene de attributen heeft.
iRvN	iRvN is de regionale samenwerkingspartner op ICT-gebied voor de gemeenten in Het Rijk van Nijmegen. Alle zeven gemeenten hebben hun ICT ondergebracht bij iRvN.
ISMS	Information Security Management System, ofwel een managementsysteem voor informatiebeveiliging. Een ISMS sluit aan bij het beleid en de strategie van je organisatie en dient geïntegreerd te worden in je huidige processen.
ISO	Internationale Organisatie voor Standaardisatie. Beheerder van wereldwijde standaarden op vele terreinen.
KPI	Kritieke prestatie-indicatoren, afgekort KPI's, zijn variabelen om prestaties van ondernemingen te analyseren.
Logisch gescheiden	De computer apparatuur is door de scheiding van het data verkeer in het computer netwerk alleen in staat met bepaalde apparatuur op hetzelfde netwerk te communiceren.
mandateren	Mandaat is de bevoegdheid om in naam van een ander te handelen, maar zonder de daarbij horende verantwoordelijkheid. Bij mandateren worden geen bevoegdheden overgedragen. De mandaatgever blijft zelf bevoegd.

MFA	Multifactor authenticatie vereist meerdere manieren om je als gebruiker kenbaar te maken. Denk daarbij aan wachtwoord, toegangscode, vingerafdruk, irisscan etc. Dat kunnen er meer dan twee zijn.
NCSC	Nationaal Cyber Security Centrum is een publiek-private Nederlandse organisatie die de weerbaarheid van de Nederlandse samenleving wil vergroten oa door het publiceren van beveiligingsadvieze.
Prince2 (PSA, PEA)	Prince2 is een project management methode waarin de begrippen project startarchitectuur en project einde thuis horen. Prince is een methode die bij de overheid gangbaar is.
Plan, do, check en act	Een model dat ontwikkeld is om het proces van continue kwaliteitsverbetering uit te beelden.
Privacy	Persoonlijke levenssfeer
SLA	Service level agreement. Dienstenniveauovereenkomst waarin beschreven staat welk dienstverleningsniveau de opdrachtgever en opdrachtnemer hebben afgesproken.
SPF	Sender Policy Framework (afgekort SPF) is een protocol dat tot doel heeft spam te verminderen. Men hoopt e-mail spoofing en spam te verminderen door vast te stellen of de verzender van een e-mailbericht gerechtigd is te verzenden namens de vermelde afzender van het bericht.
Suwinet	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen. Digitale omgeving die bedoeld is voor overheidsorganisaties om gegevens van burgers te kunnen raadplegen met betrekking tot werk en inkomen.
Telewerken	Werken op afstand van de kantoor omgeving. Bijvoorbeeld thuis, of in de trein.
TLS	TLS zorgt door middel van de uitwisseling van certificaten voor de versleuteling van gegevens tijdens het transport tussen internetsystemen
TOTP	Time-based One-time Password. Eenmalig tijdgebonden wachtwoord. Meestal een code gegenereerd in een app gebruikt als tweede factor bij het inloggen
Whitelist	Toegang verlenen op basis van een positieve lijst. Dat wil zeggen dat je toegang krijgt tot iets als op de lijst staat dat de verbinding toegestaan is. Het alternatief (blacklist, wordt vaker gebruikt) is dat je toegang krijgt tenzij op de lijst staat dat de verbinding niet is toegestaan.

Van:
Verzonden: dinsdag 1 oktober 2019 09:30
Aan:
CC:
Onderwerp: RE: Responsible disclosure

Dag ,

Uiteraard akkoord dat deze pagina terugkomt.

Groeten,

Van:
Verzonden: maandag 30 september 2019 13:59
Aan:
Onderwerp: FW: Responsible disclosure

Hoi ,

Zie hier onder het gesprek met content management. Ik weet dat we het er toen over gehad hebben wat er aan privacy statement en zo op de site moest komen. Maar ik was me er niet van bewust dat het responsible disclosure statement zou verdwijnen.
Volgens mij verklaart dat waarom ik geen disclosures meer krijg. Het lijkt me goed dat er weer op te zetten.

Groet,

Van: Contentmanagement <contentmanagement@nijmegen.nl>
Verzonden: maandag 30 september 2019 13:04
Aan:
Onderwerp: RE: Responsible disclosure

Hoi ,

De nieuwe pagina is er in overleg met opgekomen. Mocht je het gevoel hebben dat er zaken ontbreken, dan graag met hem afstemmen.

Vriendelijke groet,

medewerker Gegevens | Contentmanager

Nijmegen

Gemeente Nijmegen

Van:
Verzonden: maandag 30 september 2019 12:18
Aan: Contentmanagement
CC:
Onderwerp: RE: Responsible disclosure

Hallo

Dit was de oorspronkelijke pagina:

http://www2.nijmegen.nl/content/1691460/responsible_disclosure
De tekst die daar stond gaf ook heel wat meer informatie dan de “datalek melden” pagina.
https://www.nijmegen.nl/diensten/privacy/datalek-melden/ daar staat geen informatie op over responsible disclosure.
Ik kreeg namelijk zeker 1 responsible disclosure melding per jaar in het begin, maar sindsdien niet meer. En nu snap ik ook waarom.
De tekst leek op deze tekst:
https://responsibledisclosure.nl/
Ik voeg ook een handreiking van de IBD toe met een voorbeeld tekst. Die hebben we de vorige keer volgens mij ook gebruikt. Kunnen jullie er weer een passende tekst op zetten?

Met vriendelijke groet,

Stadscontrol
Plaatsvervangend CISO

Nijmegen

Telefoon:
Email:

Van: Contentmanagement <contentmanagement@nijmegen.nl>
Verzonden: maandag 30 september 2019 10:29
Aan:
Onderwerp: RE: Responsible disclosure

Hoi beiden,

De huidige pagina ‘Datalek melden’ is de nieuwe versie van de oude responsible disclosure-pagina. Op die oude pagina stond inderdaad een link naar een PGB-key. De PGB-key is er nu ook bijgezet op de pagina ‘Datalek melden’.

Vriendelijke groet,

medewerker Gegevens | Contentmanager

Nijmegen

Gemeente Nijmegen

Van:
Verzonden: woensdag 25 september 2019 13:19
Aan: Contentmanagement;
Onderwerp: : Responsible disclosure

Hoi

Ik ben niet verantwoordelijk voor de inhoud op nijmegen.nl, ik stuur de vraag bij deze door aan de contentmanagers.

Gisteren heb ik overigens met besproken dat hier https://www.nijmegen.nl/diensten/privacy/datalek-melden/ een pgp-key toegevoegd moet worden. Werd die eerder ook op de site gebruikt dat jij weet? En zo ja, heb jij die toevallig in beheer?

Groet,

Van:
Verzonden: woensdag 25 september 2019 12:58
Aan:
Onderwerp: Responsible disclosure

Hallo ,

Volgens mij is de responsible disclosure pagina van www.nijmegen.nl verdwenen. Klopt dat? Nu snap ik ook waarom ik al een tijdje geen meldingen meer krijg. Kan die pagina weer terug? Ik kan me niet herinneren dat iemand me gevraagd heeft of die weg kon.

Met vriendelijke groet,

Stadscontrol
Plaatsvervangend CISO

Nijmegen

Telefoon:
Email:

Onderwerp: RE: Responsible disclosure

Van: Contentmanagement <contentmanagement@nijmegen.nl>
Verzonden: dinsdag 15 oktober 2019 10:08
Aan:
Onderwerp: RE: Responsible disclosure

Hoi
Dank je wel voor je reactie. Ik heb het artikel op de website uitgebreid aan de hand van het voorbeeld van Hoorn. We hebben meerdere referentiegemeenten, maar daar zitten Hoorn en Zeewolde niet bij☺.
Vriendelijke groet,

medewerker Publiekszaken

Gemeente Nijmegen

Van:
Verzonden: donderdag 10 oktober 2019 15:46
Aan: Contentmanagement <contentmanagement@nijmegen.nl>
Onderwerp: RE: Responsible disclosure
Hallo ,
De crux van de tekst over responsible disclosure zit hem er in dat je aangeeft dat je iemand niet vervolgt als ze jouw website hacken volgens bepaalde regels. En in die tekst leg je die regels dan uit. Dat zie ik nu op de site niet terug.
Dat is denk ik ook de reden waarom ik eerst wel regelmatig dit soort meldingen kreeg en nu niet meer. Nu denken hackers namelijk dat we de politie op ze af sturen als ze onze site hacken. Maar dat wil ik helemaal niet. Ik wil juist dat ze proberen onze site te hacken. Dan wordt hij namelijk gratis getest. Als ik zo`n tester in moet huren kost me dat 1000 euro per dag.
Andere gemeenten doen dat ook.
Apeldoorn: https://www.apeldoorn.nl/ter/Digitale-klokkenluidersregeling-(Responsible-Disclosure).html
Hoorn: https://www.hoorn.nl/responsibledisclosure
Zeewolde: https://www.zeewolde.nl/gemeente/responsible-disclosure_42923/
etc
Je kunt ook hier even kijken: https://www.guardian360.nl/een-responsible-disclosure-voor-elke-gemeente/
En ik stuur het document van de IBD mee. Blijkbaar was ik die de vorige keer vergeten.
Met vriendelijke groet,

Stadscontrol
Plaatsvervangend CISO

Telefoon:
Email:

Van: Contentmanagement <contentmanagement@nijmegen.nl>
Verzonden:
Aan:
CC:
Onderwerp: Responsible disclosure
Hoi ,
Omdat ‘responsible disclosure’ niet toegankelijke taal is en dat wel een uitgangspunt is van onze site heb ik er dit van gemaakt:
https://www.nijmegen.nl/diensten/privacy/beveiligings-of-datalek-melden/

We hebben ook gekeken wat andere gemeenten hiermee doen en dat (als ze het al überhaupt op hun site benoemen) komt overeen met bovenstaande.
Vriendelijke groet,

medewerker Publiekszaken

Nijmegen

Gemeente Nijmegen

Van:
Verzonden: woensdag 2 oktober 2019 13:14
Aan:
CC:
Onderwerp: : Responsible disclosure

Hallo ,
In overleg met willen we de Responsible Disclosure pagina onder Privacy hebben als zesde blokje (zie plaatje 1). Bij het klikken op dat blokje zouden we graag de volgende tekst terug zien op basis van het voorbeeld van de IBD. Zie de bijlage.
Jij had de PGP key dus die kan er bij.
Ik zou ook graag een link zien onder aan de pagina, zie plaatje 2.
Met vriendelijke groet,

Stadscontrol
Plaatsvervangend CISO

Nijmegen

Telefoon:
Email:

Van:
Verzonden: dinsdag 1 oktober 2019 09:30
Aan:
CC:
Onderwerp: RE: Responsible disclosure

Dag ,
Uiteraard akkoord dat deze pagina terugkomt.
Groeten,

Van:
Verzonden: vrijdag 28 april 2023 09:53
Aan:
CC: ; Webmaster
Onderwerp: RE: responsible disclosure

Verloopt: donderdag 27 juli 2023 00:00

Hallo

Ik heb de mail nog even teruggezocht in onze webmaster mailbox en zie dat mijn collega dit toen heeft opgepakt met een vraag aan , zie onderstaande mail van 29-6-2022.
Collega van IenA is bezig geweest met de security.txt inrichting. Deze is sinds oktober 2022 actief op 2 subdomeinen: https://app6.nijmegen.nl/.well-known/security.txt en https://mijn.nijmegen.nl/.well-known/security.txt. En hebben we overgenomen voor hoofddomein Nijmegen.nl, zie https://www.nijmegen.nl/.well-known/security.txt

Volgens internet.nl is voor het nieuwe security.txt bestand:
Niveau van vereistheid: Aanbevolen

>> mail van 29-6-2022

Hoi

Mij is niet goed duidelijk wat wil bereiken. Kan ik haar zelf bellen hierover?

We hebben namelijk al een pagina over het melden, dat er niemand meer iets meldt lijkt mij niet persé liggen aan de pagina. Ook qua prioriteit vind ik dit een lastige. Dus als ik meer hoor over wat er fout gaat/ wat zij vindt dat er verbeterd moet worden kunnen we het wellicht inplannen. (of niet)

Groetjes

Van:
Verzonden: zaterdag 25 juni 2022 09:23
Aan: Webmaster <Webmaster@irvn.nl>
CC:
Onderwerp: responsible disclosure

Hallo webmaster,

In de communicatie van IBD kwam laatst een opmerking voorbij over security.txt. Na wat zoeken kwam ik onderstaande tegen:

https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf
Security.txt blijkt (als ik het goed begrijp) een toegevoegd bestandje te zijn op de website waarin voor iemand die een disclosure melding wil doen relevante informatie staat. Nu dacht ik dat wij responsible disclosure vrij aardig op orde hebben maar we krijgen geen meldingen (eerste paar jaar een paar daarna niets meer). Zou jij met deze toolkit in de hand een voorstel kunnen doen om het makkelijker en meer uitnodigend te maken om een disclosure melding te doen?

Met vriendelijke groet,

Stadscontrol
CISO
<<

Met vriendelijke groet,

Van:
Verzonden: woensdag 26 april 2023 15:49
Aan:
CC:
Onderwerp: FW: responsible disclosure

Hallo ,

Onderstaande mail heb ik een hele tijd geleden naar Webmaster IRVN gemaild. Naar aanleiding van een vraag die ik vandaag kreeg ben ik gaan kijken wat het antwoord op deze vraag was maar dat heb ik niet kunnen vinden. Als het goed is zou mijn mail destijds jou bereikt moeten hebben. Volgens mijn informatie ben jij de webmaster. Kun jij kijken of je mij een antwoord gestuurd hebt? Zo nee, zou je dan alsnog een antwoord kunnen sturen?

Met vriendelijke groet,

Stadscontrol
CISO

Nijmegen

Telefoon:
Email:

Van:
Verzonden: zaterdag 25 juni 2022 09:23
Aan: Webmaster <Webmaster@irvn.nl>
CC:
Onderwerp: responsible disclosure

Hallo webmaster,

In de communicatie van IBD kwam laatst een opmerking voorbij over security.txt. Na wat zoeken kwam ik onderstaande tegen:
https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf
Security.txt blijkt (als ik het goed begrijp) een toegevoegd bestandje te zijn op de website waarin voor iemand die een disclosure melding wil doen relevante informatie staat. Nu dacht ik dat wij responsible disclosure vrij aardig op orde hebben maar we krijgen geen meldingen (eerste paar jaar een paar daarna niets meer). Zou jij met deze toolkit in de hand een voorstel kunnen doen om het makkelijker en meer uitnodigend te maken om een disclosure melding te doen?

Met vriendelijke groet,

Stadscontrol
CISO

Nijmegen

Telefoon:
Email:

Wat moet er in het informatiebeveiligingsbeleid (uitwerking) 2021

In 2020 is het Informatiebeveiligingsbeleid niet herzien, hangende een evaluatie van het beleid. De manier van het evalueren van het beleid wordt ontwikkeld maar is nog niet bruikbaar. Ondertussen zijn er de nodige ontwikkelingen geweest die hun weerslag moeten vinden in het informatiebeveiligingsbeleid en zal een herziening dit jaar moeten plaatsvinden. Dit jaar betekent dat de nieuwe tekst voor de zomer af zou moeten zijn.

Uit verschillende bronnen heb ik in de loop van het jaar punten verzameld die verwerkt zouden moeten worden in het nieuwe beleid.

Het verzoek is of wij het herzien van het informatiebeveiligingsbeleid gezamenlijk op kunnen pakken op een manier die voorkomt dat een persoon onevenredig belast wordt en toch een product oplevert waar wij achter kunnen staan.

Accountant

Wachtwoordbeleid
Wachtwoordbeleid in lijn met best practices en praktijk:

Op basis van document inspectie is vastgesteld dat Nijmegen in het informatiebeveiligingsbeleid de wachtwoordvereisten heeft opgenomen, echter zijn de volgende wachtwoord configuratie instellingen (nog) niet opgenomen:
•Accountlock-out(bestaande uit het aantal minuten, aantal pogingen, en de reset van de lock-out pogingen);

•Wachtwoordhistorie;

•Minimale wachtwoord lengte.

Het verdient aanbeveling om het informatiebeveiligingsbeleid 2019 te updaten en hierbij het wachtwoordbeleid aan te scherpen naar de Deloitte good-practice richtlijnen:
•Wachtwoordhistorie: 14-24 of meer wachtwoorden (afhankelijk van normale eindgebruiker of beheeraccount);

•Minimum wachtwoordlengte: 8-14 karakters (afhankelijk van normale eindgebruiker of beheeraccount);

•Duurlock-out: 30 minuten;

•Aantal pogingen alvorens lock-out: 3;

•Reset aantal pogingen lock-out: 1440 minuten.

In aanvulling op bovenstaande wachtwoord configuratie instellingen adviseren wij om de two-factor authentication (2FA) onderdeel uit te laten maken van het ‘onderzoekwachtwoorden’ van de gemeente zodat de implementatie hiervan gerealiseerd kan worden.

MDM en nieuwe werkplek.
Wat kan wel en wat kan niet met de nieuwe inrichting. Hoe werkt de medewerker op welke locatie (gerelateerd aan corona).

Opleiding en afspraken met medewerkers
Continue opleiding en bijscholing. Overleggen bewijs. Binnen 3 maanden na in dienst de eerste module afgerond. Communicatie naar medewerker over wat van hem/haar verwacht wordt in functie.

Gebruik social media
Zie Z&I afspraken die voorstelde

Rollen en taken
iRvN, hoe houden we contact, ook bij een crisis (koppeling met crisis proces). Hoe werken we samen. Wat is de verantwoordelijkheid van de gemeente/ proceseigenaren. Zie ook de opmerkingen van de accountant over het afronden van processen.

De iRvN heeft een belangrijke rol in het realiseren van de doelstellingen in het informatiebeveiligingsbeleid. Deze rol is echter minimaal beschreven in het uitwerkingsdocument, alsmede is er een minimale beschrijving van de verantwoording van de taken en verantwoordelijkheden door de iRvN

informatiebeveiligingsbeleid organisatie breed toe te passen. Advies is om het informatiebeveiligingsbeleid te verbreiden naar het volledige aspect van informatieveiligheid in plaats de focus op de AVG.

Beschrijving vernieuwde privacy ambassadeurs, SO?

Logging en rapportage
SIEM-EWS en applicaties: wat willen we voor de verschillende soorten logging, wat willen we kunnen zien per soort (voor auditor, accountant, maar ook dreiging, inzage)

Crisisteam
Gerelateerd aan het crisisproces: taken in vredestijd, oefenen, casusbespreking

ENSIA Audit:
Suwinet RMC en DKD inlezen toevoegen.

Documentatie op orde voor de audit. Controle door het jaar heen inplannen en uitvoeren. Incidentmanagement proces gemeente intern, aansluitend op de incidentmanagement processen van de iRvN, maken en naar verwijzen.

Informatiebeveiligingsplan
Beleid + cybermanager => informatiebeveiligingsplan
Welke vorm heeft dit plan? Is hier een apart plan voor nodig. Hoe verhoudt zich dit tot het controle plan van de FG.

Evaluatie beleid (en plannen)
Proces wanneer en op basis van welke informatie. In samenhang met andere

Input vanuit direct betrokkenen
Ontwikkel I&A
AVG proof project
FG/PO/SO/CISO en privacy ambassadeurs
Evaluatie IB (als dat lukt)
Kwaliteitsmedewerkers stelsels (BRP, SUWI, BAG/BGT/BRO, DigiD)

WPG noemen
wachtwoordeisen verscherpen
Logging beleid op basis van vertrouwelijkheid bewaartermijn 5 jr (Nen7513)
NIS2 etc
Veilig mailen beleid nav NEN 7516